TSA Registered Traveler

Appendix C:
Minimum Required RT Security Standards and Procedures for Assessing Compliance with RT Security Standards

Version 3.1, January 2008

Transportation Security Administration

RT Registered Traveler™

Appendix C: Minimum Required RT Security Standards and Procedures for Assessing Compliance with RT Security Standards

Minimum Required RT Security Standards

The Minimum Required RT Security Standards were created to provide Service Providers (SPs) with the most technically sound and broadly applicable set of security controls for RT information and information systems. A variety of sources were considered during the development of this standard, including security controls from NIST SP 800-53, the AICPA Generally Accepted Privacy Principles, and others from the audit, financial, healthcare, and privacy communities. It is the responsibility of the SPs to implement the controls correctly and to demonstrate the effectiveness of the controls in satisfying their stated security requirements.

The following table of security controls provides a range of safeguards and countermeasures for information systems. The security controls are organized into *families* for ease of use in the control selection and specification process. Each family contains security controls related to the security functionality of the family. A standardized, two-character identifier is assigned to uniquely identify each control family. To uniquely identify each control, a numeric identifier is appended to the family identifier to indicate the number of the control within the control family. Many of the controls in the standards were derived from NIST SP 800-53. Therefore, for consistency purposes, the unique identifiers for these controls have not been changed. For example, the control identifiers in the Access Control (AC) family jump from AC-14 to AC-17 in this document (NIST SP 800-53 controls AC-15 and AC-16 are not applicable to this standard).

While SPs are required to follow the Minimum Required RT Security Standards, there is flexibility in how SPs apply the standards. Unless otherwise specified by TSA, the standard generally allows some latitude in the implementation of the controls. Consequently, the application of this standard by SPs can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the definition of *adequate security* for information systems. When assessing SP compliance with this guidance, auditors, evaluators, and/or assessors should consider the intent of the security concepts and principles articulated within the standard and how the SP applied the guidance in the context of its specific mission responsibilities, operational environments, and unique organizational conditions.

Control Number	Control Description
Access Control Class: Operational	
AC-1 Access Control Policy And Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, 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.
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 at least 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 Login Attempts	The information system enforces a predefined limit of consecutive invalid access attempts by a user during a predefined time period. The information system automatically locks the account/node for a predefined time period when the maximum number of unsuccessful attempts is exceeded.
AC-8 System Use Notification	The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing an RT information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited; 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.
AC-9 Previous Logon Notification	The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

Control Number	Control Description
AC-10 Concurrent Session Control	The information system limits the number of concurrent sessions for any user.
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 20 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 Without 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: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) documents, monitors, and controls wireless access to the information system. Appropriate organizational officials authorize the use of wireless technologies.
AC-19 Access Control For Portable And Mobile Devices	The organization: (i) establishes usage restrictions and implementation guidance for portable and mobile devices; and (ii) documents, monitors, and controls device access to organizational networks. Appropriate organizational officials authorize the use of portable and mobile devices.
AC-20 Personally Owned Information Systems	The organization restricts the use of personally owned information systems for official RT business involving the processing, storage, or transmission of RT information.

Control Number	Control Description
Awareness And Training Class: Operational	
AT-1 Security Awareness And Training Policy And Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, 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.
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 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 annually 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.
Family: Audit And Accountability Class: Technical	
AU-1 Audit And Accountability Policy And Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, 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.
AU-2 Auditable Events	The information system generates audit records for the following events: All successful and unsuccessful attempts to access RT networks, network devices, software applications, and systems; activities that might modify, bypass, or negate IT security safeguards; and security-relevant actions associated with processing.
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 Description
AU-5 Audit Processing	In the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes a predefined course of action.
AU-6 Audit Monitoring, Analysis, And Reporting	The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.
AU-7 Audit Reduction And Report Generation	The information system provides an audit reduction and report generation capability.
AU-8 Time Stamps	The information system provides time stamps for use in audit record generation.
AU-9 Protection Of Audit Information	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.
AU-10 Non-repudiation	The information system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).
AU-11 Audit Retention	The organization retains audit logs on-line by the system/network administrator for a predefined number of days and archived off-line for a predefined period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
Configuration Management Class: Operational	
CM-1 Configuration Management Policy and procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, 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.
CM-2 Baseline Configuration And System Component Inventory	The organization develops, documents, and maintains a current, baseline configuration of the information system, an inventory of the system's constituent components, and relevant ownership information.
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.

Control Number	Control Description
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 physical and logical access restrictions associated with changes to the information system and generates, retains, and reviews records reflecting all such changes.
CM-6 Configuration Settings	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.
CM-7 Least Functionality	The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of all unnecessary functions, ports, protocols, and/or services.
Contingency Planning Class: Operational	
CP-1 Contingency Planning Policy And Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, 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.
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	The organization tests the contingency plan for the information system annually using table top exercises to determine the plan's effectiveness and the organization's readiness to execute the plan. Appropriate officials within the organization review the contingency plan test results and initiate corrective actions.

Control Number	Control Description
CP-5 Contingency Plan Update	The organization reviews the contingency plan for the information system annually 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-8 Telecommunications Services	The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable.
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 daily (incremental) and weekly (full) 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 Class: Technical	
IA-1 Identification And Authentication Policy And Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, 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.
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: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after a predefined period of inactivity; and (vi) archiving user identifiers.

Control Number	Control Description
IA-5 Authenticator Management	The organization manages information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and (iii) changing default authenticators upon information system installation.
IA-6 Authenticator Feedback	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
IA-7 Cryptographic Module Authentication	For authentication to a cryptographic module, the information system employs authentication methods that meet the Triple Data Encryption Standard.
Incident Response Class: Operational	
IR-1 Incident Response Policy And Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, 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.
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 annually.
IR-3 Incident Response Testing	The organization tests the incident response capability for the information system annually using [Assignment: organization-defined tests and exercises] 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, in accordance with the RT Standards.
IR-7 Incident Response Assistance	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 Number	Control Description
Family: Maintenance Class: Operational	
MA-1 System Maintenance Policy And Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, 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.
MA-2 Periodic Maintenance	The organization schedules, performs, and documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.
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 for key information system components within a predefined period of a failure.
Family: Media Protection Class: Operational	
MP-1 Media Protection Policy And Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, 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.
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-3 Media Labeling	The organization affixes external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information.

Control Number	Control Description
MP-4 Media Storage	The organization physically controls and securely stores information system media, both paper and digital, based on the highest FIPS 199 security category of the information recorded on the media.
MP-5 Media Transport	The organization controls information system media (paper and digital) and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.
MP-6 Media Sanitization And Disposal	The organization: (i) sanitizes information system media, both paper and digital, prior to disposal or release for reuse; (ii) tracks, documents, and verifies media sanitization actions; and (iii) periodically tests sanitization equipment and procedures to ensure correct performance.
Physical And Environmental Protection Class: Operational	
PE-1 Physical And Environmental Protection Policy And Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, 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.
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 annually.
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.

Control Number	Control Description
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 Logs	The organization maintains a visitor access log to facilities (except for those areas within the facilities officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the access logs based on a predefined schedule.
PE-9 Power Equipment And Power	The organization protects power equipment and power cabling for the information system from damage and destruction.
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-17 Alternate Work Site	Individuals within the organization employ appropriate information system security controls at alternate work sites.

Control Number	Control Description
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.
Security Planning Class: Management	
PL-1 Security Planning Policy And Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, 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.
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 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.
PL-5 Privacy Impact Assessment	The organization conducts a privacy impact assessment on the information system.
PL-6 Security-related Activity Planning	The organization ensures that appropriate planning and coordination occur before conducting security-related activities affecting the information system in order to minimize the impact on organizational operations (i.e., mission, functions, image, and reputation) and organizational assets.

Control Number	Control Description
Personnel Security Class: Operational	
PS-1 Personnel Security Policy And Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.
PS-3 Personnel Screening	The organization screens individuals requiring access to organizational information and information systems before authorizing access.
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 and reviews/updates the agreements annually.
PS-7 Third-Party Personnel Security	The organization establishes personnel security requirements including security roles and responsibilities, 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.

Control Number	Control Description
Risk Assessment Class: Management	
RA-1 Risk Assessment Policy And Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, 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.
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 (including information and information systems managed/operated by external parties).
RA-4 Risk Assessment Update	The organization updates the risk assessment every 3 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	The organization scans for vulnerabilities in the information system annually or when significant new vulnerabilities affecting the system are identified and reported.
System And Services Acquisition Class: Management	
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 Design Principles	The organization designs and implements the information system using security engineering principles.

Control Number	Control Description
SA-9 Outsourced Information System Services	The organization ensures that third-party providers of information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. The organization monitors security control compliance.
SA-10 Developer Configuration Management	The information system developer creates and implements a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.
SA-11 Developer Security Testing	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 Communications Protection Class: Technical	
SC-1 System And Communications Protection Policy And Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, 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.
SC-2 Application Partitioning	The information system separates user functionality (including user interface services) from information system management functionality.
SC-3 Security Function Isolation	The information system isolates security functions from nonsecurity functions.
SC-4 Information Remnants	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.
SC-6 Resource Priority	The information system limits the use of resources by priority.
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.

Control Number	Control Description
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 a predefined period of inactivity.
SC-11 Trusted Path	The information system establishes a trusted communications path between the user and the security functionality of the system.
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 Validated Cryptography	When cryptography is employed within the information system, the cryptography complies with the RT Standards and the RTIC Technical Interoperability Specification; including FIPS 140-2 which requires the system to perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.
SC-14 Public Access Protections	For publicly available systems, 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-16 Transmission Of Security Parameters	The information system reliably associates security parameters (e.g., security labels and markings) with information exchanged between information systems.
SC-18 Mobile Code	The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of mobile code within the information system. Appropriate organizational officials authorize the use of mobile code.
SC-19 Voice Over Internet Protocol	The organization: (i) establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of VoIP within the information system. Appropriate organizational officials authorize the use of VoIP.

Control Number	Control Description
SC-20 Secure Name Lookup Service (Authoritative Source)	The information system (i.e., authoritative domain name servers) that provides the name lookup service for accessing organizational information resources to entities across the Internet provides artifacts for data origin authentication and data integrity to enable users to obtain message authentication and message integrity assurances for the information received during network-based transactions.
SC-21 Secure Name Lookup Service (Resolution)	The information system (i.e., authoritative domain name servers) that provides the name lookup service for accessing information resources to entities within the organization provides mechanisms for data origin authentication and data integrity verification and performs these services when requested by client systems.
System and Information Integrity Class: Operational	
SI-1 System And Information Integrity Policy And Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, 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.
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-6 Security Functionality Verification	The information system verifies, to the extent feasible, the correct operation of security functions [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator, shuts the system down, restarts the system] when anomalies are discovered.
SI-7 Software And Information Integrity	The information system detects and protects against unauthorized changes to software and information.
SI-8 Spam Protection	The information system implements spam protection.

Control Number	Control Description
SI-9 Information Input Restrictions	The organization restricts the information input to the information system to authorized personnel only.
SI-10 Information Accuracy, Completeness, Validity, And Authenticity	The information system checks information for accuracy, completeness, validity, and authenticity.
SI-11 Error Handling	The information system identifies and handles error conditions in an expeditious manner.
SI-12 Information Output Handling And Retention	The organization handles and retains output from the information system in accordance with organizational policy and operational requirements.
Enrollment Process **Class: N/A**	
EP-1 Biographic Information Collection	EP kiosks adhere to physical security controls to prevent individuals from compromising PII. Surveillance Around The Kiosk Is Present To Record Unauthorized Acquisition Of PII. All Public Facing Websites Must Have A Valid And Current Secure Socket Layer (Ssl) Certificate Issued By An Authorized Certificate Vendor e.g. Thwart Or Verisign. Automated Or Manual Controls Exist Which Require The Enrollment Technician To Compare Applicable Biographic Data Against U.s. Government Issued Identification Documents To Determine Whether The Rt Applicant's Biographic Data Is Accurate Prior To The Submission To CIMS. Audit Trails Exist To Uniquely Identify EP Personnel Who Verify The Accuracy Of The Biographic Data And The Validation Of Personal Identification Documents. Ep Systems Are Designed With Field Edits To Detect Inappropriate Entries. Audit Trails Exist To Uniquely Identify EP Personnel Who Authorize The Acceptance Of Biographic Data And The Validation Of Personal Identification Documents.

Control Number	Control Description
EP-2 Document Validation	EPs utilize document authentication technologies that take advantage of anti-fraud features incorporated into government-issued documents. Policies and procedures are in place to ensure EP personnel are appropriately trained to utilize validation devices and recognize counterfeit personal identification documents. System controls exist which require dual validation of personal identification documents. Audit trails exist to uniquely identify EP personnel who authorize the acceptance of biographic data and the validation of personal identification documents.
EP-3 Biometric Collection	System access controls exist which require the separation of duties between the authorization of biographic data and the collection of biometrics. Procedures are in place to monitor the chain of custody of the RT Applicant from the Document Validation to the Biometric Collection stations to ensure the biometric collection process is not compromised. Audit trails exist to uniquely identify EP personnel who collect biometric data and operator identity is verified based on a 1:1 biometric verification for each enrollment. Policies and procedures are in place to ensure EP personnel are appropriately trained to assist in the collection of RT Applicant biometrics in accordance with CIMS specifications. (Records are kept to verify training has been completed). Systematic controls are in place to ensure biometric are captured in accordance with CIMS specifications. Systematic controls are in place to ensure biometrics are captured in accordance with the RTIC Technical Interoperability Specification.

Control Number	Control Description
EP-4 Card Production And Issuance	EP systems do not have the ability to modify the payload data on the RT Card. The cards have a read only mode (once the information is created it can only be read/not altered). Unauthorized access to RT data on the card is prevented through EP initialization of card authentication keys requiring the use of crypto-graphically-based mutual authentication between the RT card and the RT Verification Provider stations prior to reading of RT data from the card. Entity issues RT cards only to individuals with 'approved' TSA security threat assessment determinations at the time of issuance. Entity issues and replaces RT cards as necessary and notifies CIMS as required by the RT Standards.
EP-5 Data Collection & Storage	Entity maintains archived electronic copies of completed enrollment forms in accordance with its written privacy policy.
EP-6 Excess Data	Entity collects excess data in accordance with the RT Standards. The entity ensures there is a logical separation between the collection of excess data and the base RT enrollment screen/form.

Control Number	Control Description
EP-7 Information Provided To And Received From Applicant	Entity informs each applicant in writing that: • The RT Program is linked to the national security environment, and TSA can suspend the program at any time if changes in the security environment warrant; • TSA considers the commencement of RT operations to occur at the point in time when an RT system is connected to CIMS and TSA begins accepting enrollment applications. When an SE or SP desires to commence RT Participant enrollment prior to receiving an initial TSA approval to provide RT services, appropriate disclosures shall notify enrollees that all such activities are not authorized by TSA, and that TSA is not responsible for loss or theft of participant enrollment data. • Payment of a fee to participate in the RT Program neither guarantees acceptance in the program nor continued enrollment status; • Collection of excess data is neither required nor endorsed by TSA; • Excess data is collected for SE and SP use only and not for TSA use; • Provision of excess data to the SP is not required for participation in the RT Program; and • Iris images may be shared with NIST for purposes of research to develop government standards for the use of iris images. Entity obtains and retains explicit digital or physical signature consenting to and understanding that TSA or its agents transmitting an "approved" or "not approved" determination of the applicant's TSA security threat assessment directly to the SP. TSA or its agents will not transmit the content of the TSA security threat assessment nor the reason behind the "approved" or "not approved" determination.
EP-8 Enrollment Conformance	Entity passes conformance testing for enrollment, and passes re-conformance testing after any major system changes.

Control Number	Control Description
Verification Process **Class: N/A**	
VP-1 Checkpoint Verification	Physical chain of custody is maintained over the RT Lane from the time the RT Participant presents themselves at the verification point to the time they are handed off to the TSO. The VP ensures that the required traveler identity verification procedures are performed in accordance with applicable TSA regulations and procedures. The unique identifier is changed with sufficient frequency to maintain the integrity of the identifier and sufficient coordination exists between the VPs and the TSOs so they can recognize the unique identifier. The VP ensures employees have undergone Criminal History Records Checks (CHRC) and Security Threat Assessment (STA), conducts ethics training, and provides for surveillance of the manned kiosks.
VP-2 Verification Controls	VP ensures there is a maximum number of biometric attempts before the RT Participant is rejected from the verification kiosk and traveler should use regular security lanes.
VP-3 Metrics	VP systems maintain sufficient metrics to measure false rejection rates. VPs monitor false rejection rates on a daily basis. VPs report metrics as specified in Section 4 of the RT Standards.
VP-4 Verification Conformance	VP passes conformance testing for verification, and passes re-conformance testing after any major system changes.
Privacy **Class: N/A**	
PR-1 Openness	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
PR-2 Collection Limitation	The entity collects personal information only for the purposes identified in the notice, describes the choices available to the individual, and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
PR-3 Purpose Specification	The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed. The entity provides all applicants the TSA Privacy Act Statement at the time of enrollment.

Control Number	Control Description
PR-4 Use Limitation	The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent.
PR-5 Data Quality	The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
PR-6 Individual Participation	The entity provides individuals with access to their personal information for review and update and has procedures to address privacy-related complaints and disputes.
PR-7 Security Safeguards	The entity protects personal information against such risks as loss, unauthorized access, destruction, use, modification, or disclosure of data.
PR-8 Accountability	The entity monitors compliance with its privacy policies and procedures.
Registered Traveler Class: N/A	
RT-1 Security Status	The entity transmits employee information as required for key personnel. The entity processes daily updates to card revocation lists as provided by the CIMS.
RT-2 Updates to Biographic Information	The entity re-verifies participant identity documents and recaptures digital images of participant identity documents in accordance with EP-2 whenever a participant reports changes or updates to any of the following: • Name • Gender • Date of Birth • Citizenship Status • Place of Birth • Social Security Number • Alien Registration Number • Driver's License Number and State • Passport Number.
RT-3 RT CARD DEACTIVATION	The entity notifies CIMS within 24 hours when a card should be deactivated (when lost, stolen or malfunctioning).

Control Number	Control Description
RT-4 Interoperability	The entity does not refuse service to an RT Participant regardless of the SP with whom the RT Participant is enrolled, provided the SP is approved by TSA to provide services. The entity allows RT Participants from other SPs to use RT lines at no additional cost to the participant.
RT-5 Approval to Operate	The entity has contracted with a qualified IPA firm to perform an annual attestation of compliance with the RT Standards and required controls. The entity has obtained an attestation report and received TSA's initial approval to provide RT services before commencing operations or collection of participant enrollment data for transmission to TSA.
RT-6 Oversight	The entity includes a provision in their contract with the SE authorizing TSA oversight. The entity includes a provision in their contract with the SE allowing TSA to audit or inspect the operational and security controls over the SP's RT Program.

Procedures for Assessing Compliance with RT Security Standards

This section provides assessment procedures for the security controls defined in the RT Security Standards. The assessment procedures are organized by families similar to the security controls in the RT Security Standards. Each procedure consists of multiple procedural statements, which are used in assessing some particular aspect of a security control.

In preparation for the assessment of security controls, a significant amount of background information should be assembled and made available to the assessors or assessment team. The organization should identify and arrange access to: (i) elements of the organization responsible for developing, documenting, disseminating, reviewing, and updating all security policies and associated procedures for implementing the policies; (ii) the security policies for the information system and any associated implementing procedures; (iii) individuals or groups responsible for the development, implementation, operation, and maintenance of security procedures; (iv) any materials (e.g., security plans, records, schedules, assessment reports, after-action reports, agreements, accreditation packages) associated with the implementation of security procedures and operations; and (v) the number/percentage of objects to be assessed by category. The preparation and availability of essential documentation as well as access to key organizational personnel are paramount to a successful assessment of the information system security controls.

Procedures for Assessing Compliance with RT Security Standards

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Acess Control Class: Operational		
Control Number: AC-1 ACCESS CONTROL POLICY AND PROCEDURES		
	None	**Examine** organizational records or documents to determine if access control policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. **Examine** the access control procedures to determine if the procedures are sufficient to address all areas identified in the access control policy and all associated access controls. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access control policy and procedures control is implemented. **Examine** the access control policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies, regulations, standards, and guidance. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the organization consistently applies the access control policy and procedures on an ongoing basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access control policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AC-2 ACCOUNT MANAGEMENT		
Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts.	(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 [Assignment: organization-defined time period for each type of account]. (3) The information system automatically disables inactive accounts after [Assignment: organization-defined time period]. (4) The organization employs automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals are notified.	**Examine** organizational records or documents to determine if the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures. **Examine** organizational records or documents to determine if the organization conducts information system account reviews within the prescribed organization-defined frequency and any required actions as a result of the reviews have occurred in accordance with established procedures. **Examine** selected active user accounts to determine if the organization followed procedures to establish and activate the user accounts and completed any organization-required documentation. **Examine** a list of recently disabled information system accounts and compare to selected system-generated records with user IDs and last login date for each account to determine if the last log-in date is beyond the date that the account is disabled. **Examine** a list of recently separated or terminated employees to determine if the organization removed accounts for these individuals according to established procedures and completed any organization-required documentation. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the account management control is implemented. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the organization consistently manages information system accounts on an ongoing basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the account management control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents to determine if the organization employs automated mechanisms to support information system account management functions and how those mechanisms are implemented. **Test** selected automated mechanisms within the information system that support the account management functions to determine if the mechanisms are operating as intended and the account management activities are properly conducted. **Examine** organizational records or documents to determine if temporary and emergency accounts are automatically terminated after [organization-defined time period] for each type of account.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AC-2 ACCOUNT MANAGEMENT		
The organization ensures that account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know changes.		**Examine** the information system configuration settings to determine if the settings are set to automatically terminate temporary and emergency accounts after [organization-defined time period]. **Examine** organizational records or documents to determine if any temporary or emergency accounts have not been terminated after [organization-defined time period]. **Test** the information system to determine if temporary and emergency accounts are automatically terminated after exceeding a set time period. **Examine** organizational records or documents to determine if inactive accounts on the information system are automatically disabled after [organization-defined time period]. **Examine** the information system configuration settings to determine if the settings are set to automatically disable inactive accounts after [organization-defined time period]. **Examine** organizational records or documents to determine if inactive accounts on the information system are automatically disabled after [organization-defined time period]. **Examine** the information system configuration settings to determine if the settings are set to automatically disable inactive accounts after [organization-defined time period]. **Examine** organizational records or documents to determine if any inactive accounts on the information system have not been disabled after [organization-defined time period], (i.e., if the last login date exceeds the organization-defined time period for disabling inactive accounts). **Test** the information system to determine if inactive accounts are automatically disabled after exceeding [organization-defined time period]. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the organization employs automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and that appropriate individuals are notified of these occurrences. **Test** selected automated mechanisms within the information system that support the account management auditing and notification functions to determine if: (i) the mechanisms are operating as intended; (ii) each of the account actions identified produce accurate and informative audit records; and (iii) each action, as required by the account management procedures, results in notification of appropriate individuals.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AC-3 ACCESS ENFORCEMENT		
Access control policies (e.g., identity-based policies, role-based policies, ruled-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used meets the Advanced Encryption Standard requirements for data at rest.	(1) The information system ensures that access to security functions (deployed in hardware, software, and firmware) and information is restricted to authorized personnel (e.g., security administrators).	**Examine** organizational records or documents to determine if user access to the information system is authorized. **Examine** access control mechanisms to determine if the information system is configured to implement the organizational access control policy. **Examine** the user access rights on the information system to determine if user privileges on the system are consistent with the documented user authorizations. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access enforcement control is implemented. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the information system consistently enforces assigned authorizations for controlling access to the system on an ongoing basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access enforcement control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents to determine if the organization explicitly defines security functions for the information system. **Examine** organizational records or documents to determine if the organization properly authorizes personnel granted access to security functions and information in accordance with organizational policy. **Test** selected accounts that have access to information system security functions to determine if the user privileges for those accounts function as documented in accordance with authorization requirements.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AC-4 INFORMATION FLOW ENFORCEMENT		
Information flow control policies and enforcement mechanisms are employed by organizations to control the flow of information between designated sources and destinations (e.g., individuals, devices) within information systems and between interconnected systems based on the characteristics of the information. Simple examples of flow control enforcement can be found in firewall and router devices that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability. Flow control enforcement can also be found in information systems that use explicit labels on information, source, and destination objects as the basis for flow control decisions (e.g., to control the release of certain types of information).		**Examine** information system interconnection agreements to determine if the agreements address: (i) the types of permissible and impermissible flow of information between systems; and (ii) the required level of authorization to allow information flow as defined in the information flow enforcement policy and procedures. **Examine** information system configuration settings to determine if controls are in place to restrict the flow of information within the system and between interconnected systems in accordance with the applicable policy, procedures, and assigned authorizations. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information flow enforcement control is implemented. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the information system consistently enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems on an ongoing basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information flow enforcement control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AC-5 SEPARATION OF DUTIES		
The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.		**Examine** organizational records or documents to determine if the information system enforces separation of duties. **Examine** organizational records or documents to determine if personnel duties requiring the use of the information system, involve functions of significant criticality or sensitivity that should be subject to control by more than one individual. **Examine** selected information system accounts to determine if any user has access authorizations or privileges that may allow the user to perform multiple conflicting security functions (e.g., (i) mission functions and distinct information system support functions should be divided among different individuals/roles; (ii) different individuals perform information system support functions such as system management, systems programming, quality assurance/testing, configuration management, and network security; and (iii) security personnel who administer access control functions should not administer audit functions). **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the separation of duties control is implemented. **Test** access control mechanisms by attempting to assign an individual user multiple, conflicting roles within the information system to determine if the system allows a single user to perform multiple functions/roles in violation of the separation of duties policy. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the information system consistently enforces assigned authorizations to support separation of duties on an ongoing basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the separation of duties control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AC-6 LEAST PRIVILEGE		
The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.		**Examine** organizational records or documents to determine if the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks. **Examine** organizational records or documents to determine what access rights/privileges the organization assigns to user tasks. **Examine** selected user accounts on the information system to determine if the access rights/privileges correspond to the authorized permissions on access documentation for specified tasks. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the least privilege control is implemented. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the information system consistently enforces the most restrictive set of rights/privileges or accesses needed by users on an ongoing basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the least privilege control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: AC-7 UNSUCCESSFUL LOGIN ATTEMPTS		
Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization.	(1) The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.	**Examine** organizational records or documents to determine if the information system in accordance with access control policy and procedures: (i) enforces the maximum number of consecutive invalid access attempts within a certain period of time; (ii) automatically enforces a limit of an organization-defined number of consecutive invalid access attempts by a user during an organization-defined time period; and (iii) enforces automatic locks on the account/node for an organization-defined time period or delays the next login prompt according to an organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded. **Examine** the information system configuration settings to determine if the information system enforces organizational policy and procedures for unsuccessful login attempts. **Test** the account lockout policy on selected user accounts by exceeding the maximum number of invalid login attempts within the organization-defined time period on the information system to determine if the information system locks the account/node. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the unsuccessful login attempts control is implemented.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AC-7 UNSUCCESSFUL LOGIN ATTEMPTS		
		Test the account lockout policy on selected accounts by establishing initial lockout by exceeding the maximum number of invalid logon attempts, and then attempt to: (i) login to the account in less than the organization defined delay lockout time period; and (ii) login to the account after the organization-defined lockout period to determine if the information system lockout/delay policy is being enforced. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the information system consistently enforces limitations on consecutive invalid access attempts on an ongoing basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the unsuccessful login attempts control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** the information system configuration settings to determine if the information system is configured to automatically lock the account/nodes until released by the administrator when the maximum number of unsuccessful attempts is exceeded. **Test** the account lockout mechanism by locking out selected accounts when exceeding the maximum number of invalid logon attempts, and then attempting to login to the accounts both before the administrator releases the locked accounts and after the administrator releases the locked accounts to determine if the information system administrator account lock release operates as intended.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AC-8 SYSTEM USE NOTIFICATION		
Privacy and security policies are consistent with applicable RT Standards System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems: (i) the system use information is available as opposed to displaying the information before granting access; (ii) there are no references to monitoring, recording, or auditing since privacy accommodations for such systems generally prohibit those activities; and (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.		**Examine** the information system use notification message to determine if the message includes the following topics: (i) the user is accessing a RT information system; (ii) information system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the information system is prohibited and subject to criminal and civil penalties; (iv) use of the information system indicates consent to monitoring and recording; and (v) appropriate privacy and security notices (based on associated privacy and security policies or summaries). **Interview** organizational personnel with access control responsibilities and **examine** organizational records or documents for approval of the information system use notification message before its use. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system use notification control is implemented. **Test** the system use notification message by accessing the login screen for the information system to determine if it remains on the screen until the user takes explicit actions to log on to the information system. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the information system consistently displays the system use notification message on an ongoing basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the system use notification control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AC-9 PREVIOUS LOGON NOTIFICATION		
		Examine the configuration settings of the information system to determine if upon successful logon, the system displays the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon. **Test** the information system by viewing a selection of user logons to the system to determine if upon successful logon, the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon are displayed. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the previous logon notification control is implemented. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the information system consistently provides users with essential logon information on an ongoing basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the previous logon notification control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: AC-10 CONCURRENT SESSION CONTROL		
		Examine the configuration settings of the information system to determine if the system limits the number of concurrent sessions for users to an organization-defined number of sessions. **Test** the concurrent session control by attempting to exceed the organization-defined number of concurrent sessions with a valid user account. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the concurrent session control is implemented. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the information system consistently limits the number of concurrent sessions on an ongoing basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the concurrent session control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AC-11 SESSION LOCK		
Users can directly initiate session lock mechanisms. The information system also activates session lock mechanisms automatically after a specified period of inactivity defined by the organization. A session lock is not a substitute for logging out of the information system.		**Examine** the configuration settings of the information system to determine if the system initiates a session lock until the user reestablishes access using appropriate identification and authentication procedures. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the session lock control is implemented. **Test** the session lock mechanism by allowing a user session to remain inactive for the organization-defined period to determine if the session lock automatically occurs on the information system and that the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the information system consistently employs a session lock capability on an ongoing basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the session lock control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: AC-12 SESSION TERMINATION		
Users can directly initiate session lock mechanisms. The information system also activates session lock mechanisms automatically after a specified period of inactivity defined by the organization. A session lock is not a substitute for logging out of the information system.		**Examine** the configuration settings of the information system to determine if the system initiates a session lock until the user reestablishes access using appropriate identification and authentication procedures. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the session lock control is implemented. **Test** the session lock mechanism by allowing a user session to remain inactive for the organization-defined period to determine if the session lock automatically occurs on the information system and that the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the information system consistently employs a session lock capability on an ongoing basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the session lock control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AC-13 SUPERVISION AND REVIEW—ACCESS CONTROL		
The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently, the activities of users with significant information system roles and responsibilities.	(1) The organization employs automated mechanisms to facilitate the review of user activities.	**Interview** selected organizational personnel with access control responsibilities to determine if the organization supervises and reviews the activities of users of the information system. **Examine** organizational records or documents to determine if unusual activity is investigated, reported to appropriate officials, and resolved. **Examine** organizational records of supervisory notices or disciplinary actions to users to determine if the organization is supervising user activities regarding the use and application of information system access controls. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the supervision and review of access control is implemented. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the organization consistently supervises and reviews user activities with respect to the enforcement and use of access controls for the information system on an ongoing basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the supervision and review of access control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities and how those mechanisms are implemented. **Examine** the configuration of the automated mechanism(s) within the information system to determine if the mechanisms support the review of user activities. **Examine** the output from the automated mechanism(s) within the information system to determine if each of the automated functions associated with the review of user activities produces accurate and informative information to support and facilitate the review of user activities with respect to access control enforcement and usage.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION		
Supplemental Guidance: The organization allows limited user activity without identification and authentication for public websites or other publicly available information systems.	(1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.	**Examine** organizational records or documents to determine what specific user actions can be performed on the information system without requiring identification and authentication. **Examine** the configuration settings of the information system to determine if the system allows users to perform certain actions on the system without identifying and authenticating to the system in accordance with access control policy and procedures. **Test** the information system by attempting to perform actions that are permitted without identification and authorization to determine if those actions can be performed in accordance with access control policy and procedures. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the permitted actions without identification and authentication control is implemented. **Test** the information system by attempting to perform actions that are not permitted for a user that has not been identified or authenticated to the information system (e.g., administrator functions). **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the organization consistently identifies actions permitted on the information system without requiring user identification or authentication on an ongoing basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the permitted actions without identification and authentication control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents to determine if the organization limits specific user actions that can be performed without identification and authentication to only the actions required to accomplish mission objectives. **Examine** the configuration settings of the information system to determine if the system allows users to perform certain mission related actions without identifying and authenticating to the system. **Test** the information system by attempting to perform actions that are not defined by the access control policy and procedures as being the minimum actions necessary to accomplish mission objectives without identification and authentication, to determine if the access controls are working as intended.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AC-17 REMOTE ACCESS		
Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). The organization permits remote access for privileged functions only for compelling operational needs.	(1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. (2) The organization uses encryption to protect the confidentiality of remote access sessions. (3) The organization controls all remote accesses through a managed access control point.	**Examine** organizational records or documents to determine if remote access is: (i) monitored on a periodic basis in accordance with organization policy; (ii) restricted through dial-up connections or protects against unauthorized connections or subversion of unauthorized connections; (iii) authorized and restricted to users with an operational need for access; and (iv) restricted to only allow privileged access based on compelling operational needs. **Examine** organizational records or documents to determine if remote access activity is being recorded in logs and reviewed periodically in accordance with the organizational policy and procedures. **Examine** organizational records or documents to determine if remote access is documented and authorized by the appropriate organization officials. **Examine** the configuration of the information system to determine if controls are employed to restrict remote access to the system. **Examine** a system-generated list of user accounts with remote access and determine if the established procedures are followed to authorize remote access for the accounts. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the remote access control is implemented. **Test** the remote access controls by attempting to gain remote access to the information system using a valid system account that does not have remote access permissions. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the organization consistently employs remote access controls for the information system on an ongoing basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the remote access control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents to determine what automated mechanisms and functions are employed to support and facilitate the monitoring and control of remote access methods. **Examine** organizational records or documents to determine if the automated mechanisms supporting the monitoring and control of remote access are effectively employed in accordance with organizational policy and procedures. **Test** the automated mechanism(s) within the information system to determine if each of the functions associated with the monitoring and control of remote access produce accurate and informative information, in accordance with remote access monitoring policy and procedures. **Interview** selected organizational personnel with access control responsibilities and **examine** the configuration of the information system to determine if the organization uses encryption to protect the confidentiality of remote access sessions.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AC-17 REMOTE ACCESS		
		Examine a remote access connection to the information system to determine if the connection requires the use of encryption and encryption is actually employed. **Interview** selected organizational personnel with access control responsibilities and **examine** the configuration of the information system to determine if the organization controls remote access through a managed access control point. **Test** remote access controls by attempting to connect remotely to the information system without connecting through the managed access control point to determine if remote access can be achieved without following organizational policy and procedures.
Control Number: AC-18 WIRELESS ACCESS RESTRICTIONS		
NIST Special Publication 800-48 provides guidance on wireless network security.	(1) The organization uses authentication and encryption to protect wireless access to the information system.	**Examine** organizational records or documents to determine if the organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; (ii) documents, monitors, and controls wireless access to the information system; and (iii) authorizes the use of wireless technologies. **Examine** organizational records or documents to determine if the organization tracks and monitors wireless access and usage in accordance with organizational policy and procedures. **Examine** organizational records or documents to determine if wireless users have been authorized to access the information system. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the wireless access restrictions control is implemented. **Test** wireless access controls by attempting to access the information system through an unauthorized wireless connection to determine if the system is adequately protected from unauthorized wireless access. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the organization consistently employs wireless access restrictions an ongoing basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the wireless access restrictions control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** the configuration of the information system to determine if wireless access to the system is only permitted through the use of authentication with encryption. **Test** the wireless access restrictions by attempting to access the information system: (i) using an encrypted connection without authenticating to the system; and (ii) with a valid authentication mechanism over an unencrypted connection to determine if the access restrictions operate as intended.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES		
Portable and mobile devices (e.g., notebook computers, workstations, personal digital assistants) are not allowed access to organizational networks without first meeting organizational security policies and procedures. Security policies and procedures might include such activities as scanning the devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless).	(1) The organization employs removable hard drives or cryptography to protect information residing on portable and mobile devices.	**Examine** organizational records or documents to determine if: (i) the organization establishes and documents restrictions and implementation guidance for portable and mobile devices; (ii) the organization monitors and controls the use of portable and mobile devices; and (iii) appropriate organizational officials authorize the use of portable and mobile devices and device access to organizational information systems. **Interview** selected organizational personnel with access to the information system and **examine** organizational records or documents detailing the use of portable and mobile devices to determine if personnel are complying with the usage restrictions and applying the implementation guidance on the use of portable and mobile devices in accordance with organization policy and procedures. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access control for portable and mobile devices is implemented. **Test** the use of portable and mobile devices to access organizational information systems by attempting to connect an unauthorized portable or mobile device to an organizational information system to determine if organizational personnel can identify the unauthorized device. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the organization consistently implements access controls for portable and mobile devices on an ongoing basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access control for portable and mobile devices are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents to determine if the organization employs removable hard drives or cryptography to protect information on portable and mobile devices. **Interview** selected organizational personnel who use authorized portable or mobile devices to determine if they employ removable hard drives or cryptography to protect the information on the devices. **Examine** selected authorized portable or mobile devices to determine if the devices employ removable hard drives or cryptography to protect the information on the devices.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AC-20 PERSONALLY OWNED INFORMATION SYSTEMS		
The organization establishes strict terms and conditions for the use of personally owned information systems when accessing RT information systems. The terms and conditions should address, at a minimum: (i) the types of applications that can be accessed from personally owned information systems; (ii) the maximum FIPS 199 security category of information that can processed, stored, and transmitted; (iii) how other users of the personally owned information system or individuals with potential access to the information system, are prevented from accessing RT information; (iv) the use of virtual private networking (VPN) and firewall technologies; (v) the use of and protection against the vulnerabilities of wireless technologies; (vi) the use of adequate physical security controls; (vii) the use of malicious code protection software;		**Examine** organizational records or documents to determine if the use of a personally owned information system meets the following minimum requirements as defined by the access control policy and procedures regarding: (i) the types of applications that can be accessed from personally owned information systems; (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted; (iii) how other users of the personally owned information system will be prevented from accessing RT information; (iv) the use of virtual private networking (VPN) and firewall technologies; (v) the use of and protection against the vulnerabilities of wireless technologies; (vi) the maintenance of adequate physical security controls; (vii) the use of malicious code protection software; and (viii) how often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, malicious code definitions, firewall version updates, malicious code protection definitions). **Interview** selected organizational personnel with access to the information system to determine if the personnel are adhering to the restrictions on the use of personally owned information systems for processing, storing, or transmitting RT I information in accordance with access control policy and procedures. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personally owed information systems control is implemented. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the organization consistently employs restrictions on the use of personally owned information system on an ongoing basis. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personally owned information systems control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Awareness And Training **Class: Operational**		
Control Number: AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES		
The security awareness and training policy and procedures are consistent with applicable RT Standards. The security awareness and training policy can be included as part of the general information security policy for the organization.		**Examine** organizational records or documents to determine if security awareness and training policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. **Examine** the security awareness and training policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. **Examine** the security awareness and training procedures to determine if the procedures are sufficient to address all areas identified in the security awareness and training policy and all associated security awareness and training controls. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security awareness and training policy and procedures control is implemented. **Examine** the security awareness and training policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies regulations, standards, and guidelines. **Interview** selected organizational personnel with security awareness and training responsibilities and **examine** organizational records or documents to determine if the organization consistently applies the awareness and training policy and procedures on an ongoing basis. **Interview** selected organizational personnel with security awareness and training responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security awareness and training policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AT-2 SECURITY AWARENESS		
The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access.		**Examine** organizational records or documents to determine if: (i) security awareness instruction is provided to all users; (ii) records include the type of instruction received and the date completed; and (iii) initial and refresher instruction is provided in accordance with organization-defined frequency, at least annually. **Examine** security awareness instructional materials to determine if the materials address the specific requirements of the organization and the information systems to which personnel have authorized access. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security awareness control is implemented. **Interview** selected organizational personnel with security awareness and training responsibilities and **examine** organizational records or documents to determine if the organization consistently conducts security awareness instruction on an ongoing basis. **Interview** selected organizational personnel with security awareness and training responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security awareness control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: AT-3 SECURITY TRAINING		
The organization determines the appropriate content of security training based on the specific requirements of the organization and the information systems to which personnel have authorized access.		**Examine** organizational records or documents to determine if the organization identifies personnel with significant information system security responsibilities and documents those roles and responsibilities. **Examine** organizational records or documents to determine if: (i) the organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system; (ii) records include the type of security training received and the date completed; and (iii) the organization provides initial and refresher training in accordance with organization-defined frequency. **Examine** the security training material for the selected roles and responsibilities to determine if the material addresses the procedures and activities necessary to fulfill those roles and responsibilities. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security training control is implemented.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AT-3 SECURITY TRAINING		
In addition, the organization ensures system managers, system administrators, and other personnel having access to system-level software have adequate technical training to perform their assigned duties.		**Interview** selected organizational personnel with security awareness and training responsibilities and **examine** organizational records or documents to determine if the organization consistently conducts security training on an ongoing basis. **Interview** selected organizational personnel with security awareness and training responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security training control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: AT-4 SECURITY TRAINING RECORDS		
		Examine the information system configuration to determine if the organization allocates sufficient audit record storage capacity and establishes configuration settings to prevent such capacity from being exceeded. **Test** the information system configuration to determine if the organization allocates sufficient audit record storage capacity and establishes configuration settings to prevent such capacity from being exceeded by artificially generating enough auditable events to create a number of audit records to exceed the storage capacity. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit storage capacity control is implemented. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if the organization consistently allocates sufficient audit storage capacity on an ongoing basis. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the audit storage capacity control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Family: Audit and Accountability **Class: Technical**		
Control Number: AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES		
The audit and accountability policy and procedures are consistent with applicable RT Standards. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general, and for a particular information system, when required.		**Examine** organizational records or documents to determine if audit and accountability policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. **Examine** the audit and accountability policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. **Examine** the audit and accountability procedures to determine if the procedures are sufficient to address all areas identified in the audit and accountability policy and all associated audit and accountability controls. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit and accountability policy and procedures control is implemented. **Examine** the audit and accountability policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies, regulations, standards, and guidance. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if the organization consistently applies the audit and accountability policy and procedures on an ongoing basis. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the audit and accountability policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: AU-2 AUDITABLE EVENTS		
The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance.	(1) The information system provides the capability to compile audit records from multiple components throughout the system into a system wide (logical or physical), time-correlated audit trail.	**Examine** organizational records or documents and the information system configuration settings to determine if the system generates audit records for the organization-defined auditable events. **Test** the information system by attempting to perform actions that are configured to generate an audit record. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the auditable events control is implemented.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AU-2 AUDITABLE EVENTS		
Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents.	(2) The information system provides the capability to manage the selection of events to be audited by individual components of the system.	**Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if the information system consistently generates audit records for auditable events on an ongoing basis. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the auditable events control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with audit and accountability responsibilities to determine if the information system compiles audit records into a system wide (logical or physical), time-correlated audit trail. **Examine** the information system audit trail to determine if the system accurately compiles audit records from multiple components. **Test** the information system audit trail to determine if it accurately compiles audit records from multiple components by artificially launching auditable events that are configured to generate audit records assigned to different component collection points. **Examine** organizational records or documents to determine if the information system provides the capability to manage the selection of events to be audited by individual components of the system. **Test** the capability of information system to manage the selection of events to be audited by configuring different sets of events to be audited by artificially launching auditable events that are configured to generate audit records for the selected events and ensuring they indeed generate audit records.
Control Number: AU-3 CONTENT OF AUDIT RECORDS		
Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) subject identity; and (v) the outcome (success or failure) of the event.	(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.	**Examine** organizational records or documents to determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. **Test** the content of audit records by attempting to perform actions that are configured to generate audit records to determine if the audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the content of audit records control is implemented. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if the information system consistently captures sufficient audit information to support organizational audit and accountability requirements on an ongoing basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AU-3 CONTENT OF AUDIT RECORDS		
	(2) The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.	**Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the content of audit records control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents to determine if 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. **Test** the information system capability to include additional, more detailed information in the audit records for audit events by changing the audit configuration settings to add additional information and by performing actions that create audit records to ensure the additional information is captured. **Examine** organizational records or documents to determine if the information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system. **Test** the information system capability to determine if the content of audit records generated by individual components throughout the system are centrally managed by artificially generating auditable events at different components and utilizing the central management functionality.
Control Number: AU-4 AUDIT STORAGE CAPACITY		
		Examine the information system configuration to determine if the organization allocates sufficient audit record storage capacity and establishes configuration settings to prevent such capacity from being exceeded. **Test** the information system configuration to determine if the organization allocates sufficient audit record storage capacity and establishes configuration settings to prevent such capacity from being exceeded by artificially generating enough auditable events to create a number of audit records to exceed the storage capacity. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit storage capacity control is implemented. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if the organization consistently allocates sufficient audit storage capacity on an ongoing basis. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the audit storage capacity control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AU-5 AUDIT PROCESSING		
	(1) The information system provides a warning when allocated audit record storage volume reaches [Assignment: organization-defined percentage of maximum audit record storage capacity].	**Examine** the information system configuration to determine if in the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes any additional organization-defined actions. **Test** the information system configuration to determine in the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes any additional organization-defined actions by artificially generating auditable events to cause an audit failure or excess capacity condition. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit processing control is implemented. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if the information system consistently handles audit processing anomalies including audit failures and exceeding storage capacity on an ongoing basis. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if the information system consistently handles audit processing anomalies including audit failures and exceeding storage capacity on an ongoing basis. **Examine** organizational records or documents and the information system configuration to determine if the system provides a warning when the allocated audit record storage volume reaches the organization-defined percentage of maximum audit record storage capacity. **Test** the information system configuration to determine if the system provides a warning when the allocated audit record storage volume reaches the organization-defined percentage of maximum audit record storage capacity by artificially generating auditable events to cause an excess capacity condition.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING		
	(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities. (2) The organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications.	**Examine** organizational records or documents to determine if 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. **Test** the audit monitoring, analysis and reporting process to determine if 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 by artificially generating auditable events to cause an audit failure or suspicious activity condition and monitoring how the organization reacts. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit monitoring, analysis, and reporting control is implemented. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if the organization consistently conducts audit monitoring, analysis, and reporting on an ongoing basis. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the audit monitoring, analysis, and reporting control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents and the information system configuration to determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities. **Test** the information system configuration to determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities by artificially generating auditable events and monitoring the results. **Examine** organizational records or documents and the information system configuration to determine if the organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications. **Test** the information system configuration to determine if the organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications by artificially generating auditable events and monitoring the results.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AU-7 AUDIT REDUCTION AND REPORT GENERATION		
Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.	(1) The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.	**Examine** the information system configuration to determine if the system provides an audit reduction and report generation capability. **Test** the audit reduction and report generation capability by artificially generating a sufficient number of auditable events to cause an audit reduction and report generation condition. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit reduction and report generation control is implemented. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if the information system consistently provides an audit reduction and report generation capability on an ongoing basis. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the audit reduction and report generation control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents and the information system configuration to determine if the system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria. **Test** the information system configuration to determine if the system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria by artificially generating auditable events based on selected event criteria.
Control Number: AU-8 TIME STAMPS		
Time stamps of audit records are generated using internal system clocks that are synchronized system wide.		**Examine** the information system configuration to determine if the system provides time stamps for use in audit record generation. **Test** the use of time stamps within the audit record generation capability of the information system by artificially generating an auditable event at a known time and compare the time stamp on the resulting audit record. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the time stamps control is implemented. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if the information system consistently provides time stamps on an ongoing basis. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the time stamps control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AU-9 PROTECTION OF AUDIT INFORMATION		
	(1) The information system produces audit information on hardware-enforced, write-once media.	**Examine** the information system configuration to determine if the system protects audit information and audit tools from unauthorized access, modification, and deletion. **Test** the protection of audit information and audit tools from unauthorized access, modification, and deletion by attempting to gain unauthorized access, modify, and delete audit information. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the protection of audit information control is implemented. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if the information system consistently protects audit information on an ongoing basis. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the protection of audit information control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents and the information system configuration to determine if the system produces audit information on hardware-enforced, write-once media. **Test** the information system to determine if it produces audit information on hardware-enforced, write-once media by executing the process to create the audit information on a write-once media.
Control Number: AU-10 NON-REPUDIATION		
Non-repudiation protects against later false claims by an individual of not having taken a specific action. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of having signed a document.		**Examine** the information system configuration to determine if the system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message). **Test** the information system's non-repudiation capability by: (i) demonstrating that when the non-repudiation capability is applied to a "test" action (e.g., create information, send a message, approve information[e.g., to indicate concurrence or sign a contract]), the organization can determine whether a given individual took the particular action and, when applicable, whether a given individual received something as a result of the action (e.g., received a message as a result of the action); and (ii) by demonstrating that it is not possible to alter or spoof the responsible individual's identity for a given action. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the non-repudiation control is implemented.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: AU-10 NON-REPUDIATION		
Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts, time stamps).		**Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if the information system consistently provides a non-repudiation capability on an ongoing basis. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the non-repudiation control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: AU-11 AUDIT RETENTION		
		Examine organizational records or documents to determine if the organization retains information system audit logs for an organization defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit retention control is implemented. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if the organization consistently retains audit information on an ongoing basis. **Interview** selected organizational personnel with audit and accountability responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the audit retention control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Configuration Management Class: Operational		
Control Number: CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES		
		Examine organizational records or documents to determine if the configuration management policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. **Examine** the configuration management policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. **Examine** the configuration management procedures to determine if the procedures are sufficient to address all areas identified in the configuration management policy and all associated configuration management controls. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the configuration management policies and procedures control is implemented. **Examine** the configuration management policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies, regulations, standards, and guidance. **Interview** selected organizational personnel with configuration management responsibilities and **examine** organizational records or documents to determine if the organization consistently applies the configuration management policy and procedures on an ongoing basis. **Interview** selected organizational personnel with configuration management responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the configuration management policies and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: CM-2 BASELINE CONFIGURATION AND SYSTEM COMPONENT INVENTORY		
	(1) The organization updates the baseline configuration of the information system and inventory of system components as an integral part of information system component installations. (2) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system and inventory of information system components.	**Examine** organizational records or documents to determine if the organization develops, documents, and maintains a baseline configuration of the information system which includes key architectural components and the relationship among those components. **Examine** organizational records or documents to determine if the organization develops, documents, and maintains an inventory of the hardware, software, and firmware components that compose the information system and ownership information by component. **Examine** organizational records or documents to determine if the inventory of information system components includes manufacturer, type, serial number, version number, and location (i.e., physical location and logical position within the information system architecture). **Examine** organizational records or documents to determine if the inventory of information system components designates those components required to implement and/or conduct contingency operations. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the baseline configuration and system component inventory control is implemented. **Interview** selected organizational personnel with configuration management responsibilities and **examine** organizational records or documents to determine if the organization consistently manages the baseline configuration and component inventory of the information system on an ongoing basis. **Interview** selected organizational personnel with configuration management responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the baseline configuration and system component inventory control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents to determine if the organization identifies: (i) instances that trigger baseline configuration and component inventory updates; (ii) the frequency of updates to the baseline configuration and component inventory; (iii) the dates of baseline configuration and inventory updates, a summary of the updates, and the name of the individuals performing the updates. **Examine** organizational records or documents to determine if the organization employs automated mechanisms to manage the information system baseline configuration and system component inventory functions. **Test** the automated mechanism(s) within the information system to determine if each automated function is properly configured to ensure that baseline configuration and system component inventory updates are scheduled and conducted as required. **Examine** organizational records or documents to determine if the log of baseline configuration and system component inventory updates for the information system is up-to-date, accurate, complete, and available to appropriate organizational personnel.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: CM-3 CONFIGURATION CHANGE CONTROL		
Configuration change control involves the systematic proposal, justification, test/evaluation, review, and disposition of proposed changes. The organization includes emergency changes in the configuration change control process.	(1) The organization employs automated mechanisms to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.	**Examine** organizational records or documents to determine if the organization documents and controls changes to the information system. **Examine** organizational records or documents to determine if appropriate organizational officials approve information system changes in accordance with organizational policy and procedures. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the configuration change control is implemented. **Interview** selected organizational personnel with configuration management responsibilities and **examine** organizational records or documents to determine if the organization consistently documents and controls information system configuration changes on an ongoing basis. **Interview** selected organizational personnel with configuration management responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the configuration change control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents to determine if the organization employs automated mechanisms to manage configuration changes to the information system **Test** the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: CM-4 MONITORING CONFIGURATION CHANGES		
The organization documents the installation of information system components. After the information system is changed, the organizations checks the security features to ensure the features are still functioning properly. The organization audits activities associated with configuration changes to the information system.		**Examine** organizational records or documents to determine if the organization monitors changes to the information system and identifies the types of changes monitored. **Examine** organizational records or documents to determine if the organization performs security impact analyses to assess the effects of changes to the information system. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the monitoring configuration changes control is implemented. **Interview** selected organizational personnel with configuration management responsibilities and **examine** organizational records or documents to determine if the organization consistently monitors configuration changes to the information system on an ongoing basis. **Interview** selected organizational personnel with configuration management responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the monitoring configuration changes control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: CM-5 ACCESS RESTRICTIONS FOR CHANGE		
Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. Accordingly, the organization ensures that only qualified and authorized individuals obtain access to information system components for purposes of initiating changes, upgrades, and/or modifications.	(1) The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions	**Examine** organizational records or documents to determine if the organization maintains a list of personnel authorized to access the information system for purposes of initiating changes, upgrades, and/or modifications to the system. **Examine** organizational records or documents to determine if the organization enforces physical and logical access restrictions associated with changes to the information system and generates, retains, and reviews records reflecting all such changes. **Examine** organizational records or documents identifying changes made to the information system to determine if only authorized personnel initiated, tested, approved, and implemented changes to the system. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access restrictions for change control is implemented. **Interview** selected organizational personnel with configuration management responsibilities and **examine** organizational records or documents to determine if the organization consistently enforces physical and logical access to the information system for purposes of change control on an ongoing basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: CM-5 ACCESS RESTRICTIONS FOR CHANGE		
Appropriate organizational officials approve individual access privileges.		**Interview** selected organizational personnel with configuration management responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access restrictions for change control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents to determine if the organization employs automated mechanisms to enforce access restrictions and to support auditing of the enforcement of actions. **Test** the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to enforce access restrictions and to support auditing of the enforcement of actions. **Examine** organizational records or documents to determine if the organization: (i) restricts access to automated mechanism(s) to authorized employees only; and (ii) tracks all activities performed by employees using the automated mechanism(s) to support auditing of the enforcement actions.
Control Number: CM-6 CONFIGURATION SETTINGS		
The organization documents the installation of information system components. After the information system is changed, the organizations checks the security features to ensure the features are still functioning properly. The organization audits activities associated with configuration changes to the information system.	The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.	**Examine** organizational records or documents to determine if 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. **Examine** selected information system configuration settings to determine if they are configured in accordance with the organization-defined settings. **Examine** organization documentation or records to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the configuration settings control is implemented. **Interview** selected organizational personnel with configuration management responsibilities and **examine** organizational records or documents to determine if the organization consistently applies configuration settings to the information system on an ongoing basis. **Interview** selected organizational personnel with configuration management responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the configuration settings control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: CM-6 CONFIGURATION SETTINGS		
		Examine organizational records or documents to determine if the organization employs automated mechanisms to centrally manage, apply, and verify configuration settings. **Examine** output generated by the information system to determine if the organization employs automated mechanisms to centrally manage, apply, and verify configuration settings. **Test** the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to centrally manage, apply, and verify configuration settings.
Control Number: CM-7 LEAST FUNCTIONALITY		
Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). The functions and services provided by information systems should be carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing).	(1) The organization reviews the information system [Assignment: organization-defined frequency], to identify and eliminate unnecessary functions, ports, protocols, and/or services.	**Examine** organizational records or documents to determine if the information system is configured to provide only essential capabilities and to specifically prohibit and/or restrict the use of organization-defined prohibited and/or restricted functions, ports, protocols, and/or services. **Test** the information system to determine if the identified functions, ports, protocols, and services are prohibited or restricted. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the least functionality control is implement **Interview** selected organizational personnel with configuration management responsibilities and **examine** organizational records or documents to determine if the organization consistently applies the concept of least functionality to the information system on an ongoing basis. **Interview** selected organizational personnel with configuration management responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the least functionality control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents in accordance with organization-defined frequency to determine if the organization reviews the information system to identify and eliminate unnecessary functions, ports, protocols, and/or services.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Contingency Planning Class: Operational		
Control Number: CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES		
		Examine organizational records or documents to determine if contingency planning policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. **Examine** the contingency planning policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. **Examine** the contingency planning procedures to determine if the procedures are sufficient to address all areas identified in the contingency planning policy and all associated contingency planning controls. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency planning policy and procedures control is implemented. **Examine** the contingency planning policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies regulations, standards, and guidance. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if the organization consistently applies the contingency planning policy and procedures on an ongoing basis. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the contingency planning policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: CP-2 CONTINGENCY PLAN		
	(1) The organization coordinates contingency plan development with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan	**Examine** organizational records or documents to determine if a contingency plan: (i) exists; (ii) is documented; (iii) is disseminated to appropriate elements within the organization; and (iv) is reviewed and approved by responsible officials within the organization. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities to determine if key operating elements within the organization understand the contingency plan and are ready to implement the plan. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency plan control is implemented. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if designated officials within the organization consistently review and approve the contingency plan and distribute the plan to key contingency personnel on an ongoing basis. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the contingency plan control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents to determine if the organization coordinates the contingency plan with other related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan) and if the contingency plan supports the requirements in the related plans.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: CP-3 CONTINGENCY TRAINING		
	(1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations. (2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.	**Examine** organizational records or documents to determine if the organization identifies personnel with significant contingency roles and responsibilities and documents those roles and responsibilities. **Examine** organizational records or documents to determine if the organization: (i) provides contingency training to personnel with significant contingency roles and responsibilities or personnel implementing the contingency plan; (ii) records the type of contingency training received and the date completed; and (iii) provides initial and refresher training in accordance with organization-defined frequency, at least annually. **Examine** the contingency training material for the selected roles and responsibilities to determine if the material addresses the procedures and activities necessary to fulfill those roles and responsibilities. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency training control is implemented. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if the organization consistently conducts contingency training on an ongoing basis. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the contingency training control are documented and the resulting information used to actively improve the control on a continuous basis. (1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations. **Examine** organizational records or documents to determine if the organization simulates contingency training events. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities to determine how the organization uses simulated events to improve the training process. **Test** selected simulated events to determine if organizational personnel respond as expected to the simulated crisis situation. (2) The organization employs automated mechanisms to provide a more thorough and realistic training environment. **Examine** organizational records or documents to determine if the organization employs automated mechanisms to improve contingency training. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities to determine how the automated mechanisms improve the training process. **Test** selected automated mechanisms to determine if the mechanisms are operating as intended.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: CP-4 CONTINGENCY PLAN TESTING		
There are several methods for testing contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, functional/table-top exercises).	(1) The organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan). (2) The organization tests the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations. (3) The organization employs automated mechanisms to more thoroughly and effectively test the contingency plan	**Examine** organizational records or documents to determine if the organization tests its contingency plan using the organization-defined tests and exercises in accordance with the organization-defined frequency and documents the results of the tests. **Examine** organizational records or documents to determine if the organization reviews the contingency plan test results and takes corrective actions. **Examine** organizational records or documents to determine if the contingency plan tests or exercises address key aspects of the plan and if the tests or exercises confirm that the plan objectives are met. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency plan testing control is implemented. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities to determine the overall effectiveness of the contingency plan and the readiness of the organization to execute the plan. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if the organization consistently conducts contingency plan testing on an ongoing basis. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the contingency plan testing control are documented and the resulting information used to actively improve the control on a continuous basis. (1) The organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan). **Examine** organizational records or documents to determine if the organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan). 2) The organization tests the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: CP-4 CONTINGENCY PLAN TESTING		
		Examine organizational records or documents to determine if the organization conducts contingency plan testing at the alternate processing site to familiarize contingency personnel with the facility and its resources and to evaluate the site's capabilities to support contingency operations. (3) The organization employs automated mechanisms to more thoroughly and effectively test the contingency plan. **Examine** organizational records or documents to determine if the organization employs automated mechanisms for contingency testing. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities to determine how the automated mechanisms improve the testing process. **Test** selected automated mechanisms to determine if the mechanisms are operating as intended.
Control Number: CP-5 CONTINGENCY PLAN UPDATE		
Organizational changes include changes in mission, functions, or business processes supported by the information system. The organization communicates changes to appropriate organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).		**Examine** organizational records or documents to determine if the organization updates the contingency plan in accordance with organization-defined frequency, at least annually. **Examine** the contingency plan to determine if the revised plan reflects the needed changes based on the organization's experiences during plan implementation, execution, and testing. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency plan update control is implemented. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if the organization consistently reviews and updates the contingency plan on an ongoing basis. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the contingency plan update control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: CP-6 ALTERNATE STORAGE SITES		
	(1) The alternate processing site 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) Alternate processing site agreements contain priority-of-service provisions in accordance with the organization's availability requirements. (4) The alternate processing site is fully configured to support a minimum required operational capability and ready to use as the operational site.	**Examine** organizational records or documents to determine if alternate storage site agreements are currently in place to permit storage of information system backup information. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the alternate storage site control is implemented. **Examine** the alternate storage site to determine if the site is available, accessible, and meets the requirements (including necessary equipment and supplies) to permit the storage of information system backup information. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if the organization consistently reviews and updates alternate storage site agreements on an ongoing basis. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the alternate storage sitescontrol are documented and the resulting information used to actively improve the control on a continuous basis. (1) The alternate storage site is geographically separated from the primary storage site so as not to be susceptible to the same hazards. **Examine** the contingency plan to determine if the plan identifies the primary storage site hazards. **Examine** the alternate storage site to determine if the site is sufficiently separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary site. (2) The alternate storage site is configured to facilitate timely and effective recovery operations. **Examine** the alternate storage site agreement to determine if theagreement specifies requirements to facilitate timely and effective recovery of system backup information (i.e., meeting recovery time and recovery point objectives). **Test** the alternate storage site operations to determine if the site is configured to enable timely and effective recovery of system backup information (i.e., meeting recovery time and recovery point objectives) in accordance with the provisions of alternate storage site agreement. (3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlinesexplicit mitigation actions. **Examine** the contingency plan to determine if the plan: (i) identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster; and (ii) defines explicit mitigation actions for those accessibility problems.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: CP-8 TELECOMMUNICATIONS SERVICES		
	(1) Primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the organization's availability requirements. (2) Alternate telecommunications services do not share a single point of failure with primary telecommunications services. (3) Alternate telecommunications Service Providers are sufficiently separated from primary Service Providers so as not to be susceptible to the same hazards. (4) Primary and alternate telecommunications Service Providers have adequate contingency plans.	**Examine** alternate telecommunication service agreements to determine if agreements are currently in place to permit the resumption of telecommunication services for critical mission/business functions within organization-defined time period when the primary telecommunications capabilities are unavailable. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the telecommunications services control is implemented. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if the organization consistently reviews primary and alternate telecommunications service agreements on an ongoing basis. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the telecommunicationsservices control are documented and the resulting information used to actively improve the control on a continuous basis. (1) Primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the organization's availability requirements. **Examine** primary and alternate telecommunication service agreements to determine if the agreements contain priority of service provisions in accordance with the availability requirements defined in the organization's contingency plan. (2) Alternate telecommunications services do not share a single point of failure with primary telecommunications services. **Examine** primary and alternate telecommunications service agreements and **interview** appropriate telecommunications Service Providers to determine if alternate and primary telecommunications services share a single point of failure. (3) Alternate telecommunications Service Providers are sufficiently separated from primary Service Providers so as not to be susceptible to the same hazards. **Examine** the alternate telecommunication Service Provider's site to determine if the site is sufficiently separated from the primarytelecommunication Service Provider's site so as not to be susceptible to the same hazards identified at the primary site. (4) Primary and alternate telecommunications Service Providers have adequate contingency plans. **Examine** the contingency plans from the primary and alternate telecommunication Service Providers to determine if the contingency plans are adequate.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: CP-9 INFORMATION SYSTEM BACKUP		
The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives.	(1) The organization tests backup information [Assignment: organization-defined frequency] to ensure media reliability and information integrity. (2) The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing. (3) The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software. (4) The organization encrypts backup information.	**Examine** organizational records or documents to determine if the organization defines the user-level and system-level information (including system state information) that is required to be backed up and identifies the location for storing backup information. **Examine** selected information system backup media, or selected records of backups if available, to determine if the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency and stores the backup information in designated locations in accordance with information system backup procedures. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system backup control is implemented. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if the organization consistently conducts information system backups on an ongoing basis. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system backup control are documented and the resulting information used to actively improve the control on a continuous basis. (1) The organization tests backup information [Assignment: organization defined frequency] to ensure media reliability and information integrity. **Examine** organizational records or documents including results from testing of backup operations to determine if the organization conducts testing within the organization-defined frequency, and if the testing results indicate backup media reliability and information integrity. (2) The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing. **Examine** organizational records or documents to determine if the organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing and if the use of the backup information contributes to a successful restoration of the identified functions within the information system. (3) The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software. **Examine** the storage location for backup copies of the operating system and other critical information system software to determine if the backup copies of the software are stored in a separate facility or in a fire-rated container that is not collocated with the operational software. (4) The organization encrypts backup information.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: CP-9 INFORMATION SYSTEM BACKUP		
		Examine organizational records or documents to determine if copies of backup information are encrypted. **Test** the mechanisms used to encrypt backup information on the information system by selectively decrypting selected backup files and comparing the plain text to original backup information.
Control Number: CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION		
Secure information system recovery and reconstitution to the system's original state means that all system parameters (either default or organization-established) are reset, patches are reinstalled, configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled, information from the most recent backups is available, and the system is fully tested.	(1) The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.	**Examine** organizational records or documents to determine if the organization makes available and applies mechanisms and procedures for recovery and reconstitution of the information system. **Examine** organizational records or documents to determine if the organization identifies means for capturing the information system's operational state including all system parameters, patches, configuration settings, and application/system software prior to system disruption or failure. **Examine** organizational records or documents to determine if the organization tests the information system after completion of recovery and reconstitution operations. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system recovery and reconstitution control is implemented. **Test** recovery and reconstitution mechanisms using selected components of the information system to determine if the system can be fully restored to its original operational state. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if the organization consistently conducts recovery and reconstitution operations on an ongoing basis. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system recovery and reconstitution control are documented and the resulting information used to actively improve the control on a continuous basis. (1) The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing. **Examine** organizational records or documents including results from contingency plan testing to determine if the organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Identification and Authentication Class: Technical		
Control Number: IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES		
The identification and authentication policy and procedures are consistent with applicable RT Standards and RTIC Technical Interoperability Specifications.		**Examine** organizational records or documents to determine if identification and authentication policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. **Examine** the identification and authentication policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. **Examine** the identification and authentication procedures to determine if the procedures are sufficient to address all areas identified in the identification and authentication policy and all associated identification and authentication controls. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the identification and authentication policy and procedures control is implemented. **Examine** the identification and authentication policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies regulations, standards, and guidance. **Interview** selected organizational personnel with identification and authentication responsibilities and **examine** organizational records or documents to determine if the organization consistently applies the identification and authentication policy and procedures on an ongoing basis. **Interview** selected organizational personnel with identification and authentication responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the identification and authentication policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: IA-2 USER IDENTIFICATION AND AUTHENTICATION		
Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein in accordance with applicable RT Standards and RTIC Technical Interoperability Specifications.	(1) The information system employs multifactor authentication	**Examine** organizational records or documents and the information system configuration settings to determine if the system uniquely identifies users and if authentication of user identities is accomplished through the use of passwords, tokens, or biometrics. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the user identification and authentication control is implemented. **Examine** organizational records or documents to determine if identification and authentication mechanisms are employed at the application level. **Interview** selected organizational personnel with identification and authentication responsibilities and **examine** organizational records or documents to determine if the information system consistently identifies and authenticates users on an ongoing basis. **Interview** selected organizational personnel with identification and authentication responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the user identification and authentication control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents and the information system configuration settings to determine if multifactor authentication is accomplished through some combination of passwords, tokens, or biometrics. **Test** the appropriate components of the information system to determine if a combination of passwords, tokens, or biometrics is used to employ multifactor authentication.
Control Number: IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION		
		Examine organizational records or documents and information system configuration settings to determine if the system uses either shared known information or an organizational authentication solution to identify and authenticate devices on local and/or wide area networks. **Examine** organizational records or documents to determine if the strength of the device authentication mechanism is consistent with the FIPS 199 security categorization of the information system. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the device authentication and authentication control is implemented. **Test** the information system to determine if the system identifies and authenticates specific devices before establishing connections to those devices.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION		
		Interview selected organizational personnel with identification and authentication responsibilities and **examine** organizational records or documents to determine if the information system consistently identifies and authenticates devices prior to establishing connections on an ongoing basis. **Interview** selected organizational personnel with identification and authentication responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the device identification and authentication control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: IA-4 IDENTIFIER MANAGEMENT		
Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts).		**Examine** organizational records or documents and information system configuration settings to determine if the organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after an organization-defined time period of inactivity; and (vi) archiving user identifiers. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the identifier management control is implemented. **Interview** selected organizational personnel with identification and authentication responsibilities and **examine** organizational records or documents to determine if the organization consistently manages user identifiers for the information system on an ongoing basis. **Interview** selected organizational personnel with identification and authentication responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the identifier management control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: IA-5 AUTHENTICATOR MANAGEMENT		
Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the information system: (i) validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account.		**Examine** organizational records or documents and the information system configuration settings to determine if the system protects passwords from unauthorized disclosure and modification when stored and transmitted, prohibits passwords from being displayed when entered, enforces password minimum and maximum lifetime restrictions, and prohibits password reuse for a specified number of generations. **Examine** organizational records or documents to determine if the organization establishes administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators. **Examine** organizational records or documents to determine if the organization changes default authenticators upon information system installation. **Interview** selected organizational personnel with identification and authentication responsibilities to determine if users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. **Examine** organizational records or documents to determine if the information system establishes user control of the corresponding private key and maps the authenticated identity to the user account (for PKI-based authentication). **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the authenticator management control is implemented. **Test** the information system to determine if the system protects passwords from unauthorized disclosure and modification when stored and transmitted, prohibits passwords from being displayed when entered, enforces password minimum and maximum lifetime restrictions, and prohibits password reuse for a specified number of generations. **Interview** selected organizational personnel with identification and authentication responsibilities and **examine** organizational records or documents to determine if the organization consistently manages authenticators for the information system on an ongoing basis. **Interview** selected organizational personnel with identification and authentication responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the authenticator management control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: IA-6 AUTHENTICATOR FEEDBACK		
The information system may obscure feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password). The feedback from the information system provides sufficient information for a legitimate user to understand why access is not being granted (e.g., made a keystroke mistake, forgot the password) and, at the same time, does not provide information that would allow an unauthorized user to compromise the authentication mechanism.		**Examine** organizational records or documents and information system configuration settings to determine if the system obscures feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password). **Test** the information system to determine if the feedback provides sufficient information for a legitimate user to understand why access is not granted (e.g., made a keystroke mistake, forgot the password), but does not provide information that would allow an unauthorized user to compromise the authentication mechanism. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the authenticator feedback control is implemented. **Interview** selected organizational personnel with identification and authentication responsibilities and **examine** organizational records or documents to determine if the information system consistently obscures feedback of authentication information during the authentication process on an ongoing basis. **Interview** selected organizational personnel with identification and authentication responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the authenticator feedback control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION		
		Examine organizational records or documents and information system configuration settings to determine if the system employs authentication methods for authentication to a cryptographic module that meet the standard of 128 bit 2key Triple Data Encryption Standard. **Examine** organizational records or documents to determine if the organization clearly documents authentication methods to a cryptographic module for the information system. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the cryptographic module authentication control is implemented. **Interview** selected organizational personnel with identification and authentication responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the cryptographic module authentication control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: IA-6 AUTHENTICATOR FEEDBACK		
The information system may obscure feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password). The feedback from the information system provides sufficient information for a legitimate user to understand why access is not being granted (e.g., made a keystroke mistake, forgot the password) and, at the same time, does not provide information that would allow an unauthorized user to compromise the authentication mechanism.		**Examine** organizational records or documents and information system configuration settings to determine if the system obscures feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password). **Test** the information system to determine if the feedback provides sufficient information for a legitimate user to understand why access is not granted (e.g., made a keystroke mistake, forgot the password), but does not provide information that would allow an unauthorized user to compromise the authentication mechanism. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the authenticator feedback control is implemented. **Interview** selected organizational personnel with identification and authentication responsibilities and **examine** organizational records or documents to determine if the information system consistently obscures feedback of authentication information during the authentication process on an ongoing basis. **Interview** selected organizational personnel with identification and authentication responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the authenticator feedback control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION		
		Examine organizational records or documents and information system configuration settings to determine if the system employs authentication methods for authentication to a cryptographic module that meet the standard of 128 bit 2key Triple Data Encryption Standard. **Examine** organizational records or documents to determine if the organization clearly documents authentication methods to a cryptographic module for the information system. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the cryptographic module authentication control is implemented. **Interview** selected organizational personnel with identification and authentication responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the cryptographic module authentication control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Incident Response **Class: Operational**		
Control Number: IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES		
The incident response policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular information system, when required.		**Examine** organizational records or documents to determine if incident response policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. **Examine** the incident response policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. **Examine** the incident response procedures to determine if the procedures are sufficient to address all areas identified in the incident response policy and all associated incident response controls. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident response policy and procedures control is implemented. **Examine** the incident response policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies regulations, standards, and guidance. **Interview** selected organizational personnel with incident response responsibilities and **examine** organizational records or documents to determine if the organization consistently applies incident response policy and procedures on an ongoing basis. **Interview** selected organizational personnel with incident response responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident response policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: IR-2 INCIDENT RESPONSE TRAINING		
	(1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations. (2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.	**Examine** organizational records or documents to determine if the organization identifies personnel with significant incident response roles and responsibilities and documents those roles and responsibilities. **Examine** organizational records or documents to determine if: (i) incident response training is provided to personnel with significant incident response roles and responsibilities; (ii) records include the type of incident response training received and the date completed; and (iii) initial and refresher training is provided in accordance with organization-defined frequency, at least annually. **Examine** the incident response training material for the selected roles and responsibilities to determine if the material addresses the procedures and activities necessary to fulfill those roles and responsibilities. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident response training control is implemented. **Interview** selected organizational personnel with incident response responsibilities and **examine** organizational records or documents to determine if the organization consistently conducts incident response training on an ongoing basis. **Interview** selected organizational personnel with incident response responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident response training control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents to determine if incident response training events are simulated. **Interview** selected organizational personnel with incident response responsibilities to determine how simulated events improve the training process. **Test** selected simulated events to determine if organizational personnel respond as expected to the simulated crisis situation. **Examine** organizational records or documents to determine if the organization employs automated incident response training functions. **Interview** selected organizational personnel with incident response responsibilities to determine how the automated mechanisms improve the training process. **Test** selected automated mechanisms to determine if the mechanisms are operating as intended.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: IR-3 INCIDENT RESPONSE TESTING		
	(1) The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability.	**Examine** organizational records or documents to determine if the organization tests its incident response capability using the organization-defined tests and exercises in accordance with the organization-defined frequency and documents the results of the tests. **Examine** organizational records or documents to determine if the organization reviews incident response test results and takes corrective actions. **Examine** organizational records or documents to determine if the incident response tests or exercises address key aspects of the incident response capability and if the tests or exercises confirm that the incident response objectives are met. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident response testing control is implemented. **Interview** selected organizational personnel with incident response responsibilities and **examine** organizational records or documents to determine if the organization consistently conducts incident response testing on an ongoing basis. **Interview** selected organizational personnel with incident response responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident response testing control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents to determine what incident response testing functions are automated. **Interview** selected organizational personnel with incident response responsibilities to determine how the automated mechanisms improve the testing process. **Test** selected automated mechanisms to determine if the mechanisms are operating as intended.
Control Number: IR-4 INCIDENT HANDLING		
The organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly.	(1) The organization employs automated mechanisms to support the incident handling process.	**Examine** organizational records or documents to determine if the organization implements an incident handling capability for the information system that includes preparation, detection and analysis, containment, eradication, and recovery. **Examine** organizational records or documents (or personnel engaged in incident handling activities) to determine if personnel are following designated incident handling procedures. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident handling control is implemented. **Interview** selected organizational personnel with incident response responsibilities and **examine** organizational records or documents to determine if the organization consistently conducts incident handling for the information system on an ongoing basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: IR-4 INCIDENT HANDLING		
		Interview selected organizational personnel with incident response responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident handling control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents to determine if incident handling functions are automated. **Interview** selected organizational personnel with incident response responsibilities to determine how the automated mechanisms improve the incident handling capability. **Test** selected automated mechanisms to determine if the mechanisms are operating as intended.
Control Number: IR-5 INCIDENT MONITORING		
	(1) The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.	**Examine** organizational records or documents to determine if the organization tracks and documents information system security incidents on an ongoing basis. **Examine** organizational records or documents (or personnel engaged in incident monitoring activities) to determine if personnel are following designated incident monitoring procedures. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident monitoring control is implemented. **Interview** selected organizational personnel with incident response responsibilities and **examine** organizational records or documents to determine if the organization consistently tracks and documents information system incidents on an ongoing basis. **Interview** selected organizational personnel with incident response responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident monitoring control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents to determine if incident tracking and analysis functions are automated. **Interview** selected organizational personnel with incident response responsibilities to determine how the automated mechanisms improve the incident monitoring capability. **Test** selected automated mechanisms to determine if the mechanisms are operating as intended.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: IR-6 INCIDENT REPORTING		
The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations. In addition to incident information, weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents.	(1) The organization employs automated mechanisms to assist in the reporting of security incidents.	**Examine** organizational records or documents to determine if the organization promptly reports incident information to appropriate authorities. **Examine** organizational records or documents (or personnel engaged in incident reporting activities) to determine if personnel are following designated incident reporting procedures. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident reporting control is implemented. **Interview** selected organizational personnel with incident response responsibilities and **examine** organizational records or documents to determine if the organization consistently reports information system incidents on an ongoing basis. **Interview** selected organizational personnel with incident response responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident reporting control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents to determine if incident reporting functions are automated. **Interview** selected organizational personnel with incident response responsibilities to determine how the automated mechanisms improve the incident reporting capability. **Test** selected automated mechanisms to determine if the mechanisms are operating as intended.
Control Number: IR-7 INCIDENT RESPONSE ASSISTANCE		
Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required.	(1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.	**Examine** organizational records or documents to determine if 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. **Examine** organizational records or documents (or personnel engaged in incident response support activities) to determine if personnel are following designated incident response support procedures. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident response assistance control is implemented. **Interview** selected organizational personnel with incident response responsibilities and **examine** organizational records or documents to determine if the organization consistently provides incident response support on an ongoing basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: IR-7 INCIDENT RESPONSE ASSISTANCE		
		Interview selected organizational personnel with incident response responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident response assistance control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents to determine if incident response support functions are automated. **Interview** selected organizational personnel with incident response support responsibilities to determine how the automated mechanisms improve the incident response support capability. **Test** selected automated mechanisms to determine if the mechanisms are operating as intended.
Family: Maintenance **Class: Operational**		
Control Number: MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES		
		Examine organizational records or documents to determine if the information system maintenance policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. **Examine** the information system maintenance policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. **Examine** the information system maintenance procedures to determine if the procedures are sufficient to address all areas identified in the information system maintenance policy and all associated information system maintenance controls. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system maintenance policy and procedures control is implemented. **Examine** the system maintenance policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies, regulations, standards, and guidance. **Interview** selected organizational personnel with information system maintenance responsibilities and **examine** organizational records or documents to determine if the organization consistently applies the information system maintenance policy and procedures on an ongoing basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES		
		Interview selected organizational personnel with information system maintenance responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the system maintenance policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: MA-2 PERIODIC MAINTENANCE		
Appropriate organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures. After maintenance is performed on the information system, the organization checks the security features to ensure that they are still functioning properly.	(1) The organization maintains a maintenance log for the information system that includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable). (2) The organization employs automated mechanisms to ensure that periodic maintenance is scheduled and conducted as required, and that a log of maintenance actions, both needed and completed, is up-to date, accurate, complete, and available.	**Examine** organizational records or documents to determine if the organization schedules and performs routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. **Examine** organizational records or documents to determine if the organization fully documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational periodic maintenance requirements. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the periodic maintenance control is implemented. **Interview** selected organizational personnel with information system maintenance responsibilities and **examine** organizational records or documents to determine if the organization conducts periodic maintenance on an ongoing basis. **Interview** selected organizational personnel with information system maintenance responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the periodic maintenance control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** the maintenance log to determine if the log includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable). **Examine** the automated mechanism(s) within the information system to determine if each automated function is properly configured to ensure that periodic maintenance is scheduled and conducted as required. **Examine** the log of maintenance actions to determine if the log is up to date, accurate, complete, and available.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: MA-3 MAINTENANCE TOOLS		
	(1) The organization inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications. (2) The organization checks all media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) for malicious code before the media are used in the information system. (3) The organization checks all maintenance equipment with the capability of retaining information to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized before release;	**Examine** organizational records or documents to determine if the organization approves, controls, and monitors information system maintenance tools. **Examine** approved information system maintenance tools and associated documentation to determine if the organization maintains the tools and documentation on an ongoing basis and if the processes applied are consistent with the documented maintenance procedures. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the maintenance tools control is implemented. **Interview** selected organizational personnel with information system maintenance responsibilities and **examine** organizational records or documents to determine if the organization consistently manages system maintenance tools on an ongoing basis. **Interview** selected organizational personnel with information system maintenance responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the maintenance tools control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with information system maintenance responsibilities to determine if the organization inspects all maintenance tools used by maintenance personnel for improper modifications. **Examine** organizational records or documents to determine if the organization inspects selected maintenance tools used by maintenance personnel to ensure that no improper modifications have been made. **Interview** selected organizational personnel with information system maintenance responsibilities to determine how the organization checks media containing diagnostic test programs for malicious code. **Examine** organizational records or documents to determine if the organization checks for malicious code on all media containing diagnostic test programs before use within the information system. **Examine** organizational records or documents to determine if the organization checks all maintenance equipment to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized before release. **Examine** selected maintenance equipment that cannot be sanitized to ensure that the equipment is stored in a safe and secure location within the facility or is completely destroyed.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: MA-3 MAINTENANCE TOOLS		
	if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception. (4) The organization employs automated mechanisms to ensure only authorized personnel use maintenance tools.	**Examine** organizational records or documents that indicate when maintenance equipment with organization information is removed from the facility that an organizational official explicitly authorizes the equipment removal. **Examine** organizational records or documents to determine if the organization uses automated mechanisms to control access to maintenance tools and if only authorized personnel have access to those too **Test** the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to ensure that only authorized personnel access maintenance tools.
Control Number: MA-4 REMOTE MAINTENANCE		
The organization describes the use of remote diagnostic tools in the security plan for the information system. The organization maintains maintenance logs for all remote maintenance, diagnostic, and service activities. Appropriate organization officials periodically review maintenance logs. Other techniques to consider for improving the security of remote maintenance include: (i) encryption and decryption of diagnostic communications;	(1) The organization audits all remote maintenance sessions, and appropriate organizational personnel review the audit logs of the remote sessions. (2) The organization addresses the installation and use of remote diagnostic links in the security plan for the information system.	**Examine** organizational records or documents to determine if the organization approves, controls, and monitors remotely executed maintenance and diagnostic activities. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the remote maintenance control is implemented. **Interview** selected organizational personnel with information system maintenance responsibilities and **examine** organizational records or documents to determine if the organization consistently approves, monitors, and controls remote maintenance on an ongoing basis. **Interview** selected organizational personnel with information system maintenance responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the remote maintenance control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents to determine if: (i) the organization audits all remote maintenance sessions and (ii) appropriate organizational personnel review the audit logs of the remote sessions.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: MA-4 REMOTE MAINTENANCE		
(ii) strong identification and authentication techniques, and (iii) remote disconnect verification. When remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections. If password-based authentication is used during remote maintenance, the organization changes the passwords following each remote maintenance service. For high-impact information systems, if remote diagnostic or maintenance services are required from a service or organization that does not implement for its own information system the same level of security as that implemented on the system being serviced, the system being serviced is sanitized and physically separated from other information systems before the connection of the remote access line. If the information system cannot be sanitized (e.g., due to a system failure), remote maintenance is not allowed.	(3) Remote diagnostic or maintenance services are acceptable if performed by a service or organization that implements for its own information system the same level of security as that implemented on the information system being serviced.	**Examine** organizational records or documents to determine if the organization addresses the installation and use of remote diagnostic links for the information system. **Examine** the security level of the organization performing remote diagnostic or maintenance services to determine if the services performed are at an acceptable security level. **Examine** organizational records or documents to determine if: (i) the organization maintains a list of personnel authorized to perform maintenance on the information system; and (ii) only authorized personnel have performed maintenance on the information system.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: MA-5 MAINTENANCE PERSONNEL		
Maintenance personnel have appropriate access authorizations to the information system when maintenance activities allow access to organizational information. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system.		**Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the maintenance personnel control is implemented. **Interview** selected organizational personnel with information system maintenance responsibilities and **examine** organizational records or documents to determine if the organization consistently performs an authorization of maintenance personnel on an ongoing basis. **Interview** selected organizational personnel with information system maintenance responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the maintenance personnel control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: MA-6 TIMELY MAINTENANCE		
		Examine organizational records or documents to determine if maintenance support agreements and the inventory of spare parts are sufficient to support the organization-defined list of key information system components within the organization-defined time period of failure. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the timely maintenance control is implemented. **Interview** selected organizational personnel with information system maintenance responsibilities and **examine** organizational records or documents to determine if the organization consistently obtains timely maintenance for the information system on an ongoing basis. **Interview** selected organizational personnel with information system maintenance responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the timely maintenance control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Family: Media Protection **Class: Operational**		
Control Number: MP-1 MEDIA PROTECTION POLICY AND PROCEDURES		
The media protection policy and procedures are consistent with applicable RT Standards.		**Examine** organizational records or documents to determine if the media protection policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated when organizational reviews indicate updates are required. **Examine** the media protection policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. **Examine** the media protection procedures to determine if the procedures are sufficient to address all areas identified in the media protection policy and all associated media protection controls. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media protection policy and procedures control is implemented. **Examine** the media protection policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies, regulations, standards, and guidance. **Interview** selected organizational personnel with media protection responsibilities and **examine** organizational records or documents to determine if the organization consistently applies the media protection policy and procedures on an ongoing basis. **Interview** selected organizational personnel with media protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media protection policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: MP-2 MEDIA ACCESS		
	(1) Unless guard stations control access to media storage areas, the organization employs automated mechanisms to ensure only authorized access to such storage areas and to audit access attempts and access granted.	**Examine** organizational records or documents and/or physical facilities containing media devices to determine if only authorized users have access to information in printed form or on digital media removed from the information system.
Control Number: MP-3 MEDIA LABELING		
The organization marks human-readable output appropriately in accordance with applicable policies and procedures. At a minimum, the organization affixes printed output that is not otherwise appropriately marked, with cover sheets and labels digital media with the distribution limitations, handling caveats, and applicable security markings, if any, of the information.		**Examine** organizational records or documents to determine if the organization: (i) affixes external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information; and (ii) exempts specific types of media or hardware components from labeling so long as they remain within a secure environment. **Examine** a sample of media, both storage media and system output, to determine if the media are affixed with labels indicating the distribution limitations and handling caveats of the information. **Examine** the organization-defined list of media types and hardware components that specifies types of media or hardware components that are exempt from labeling so long as they remain within a secure environment. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media labeling control is implemented. **Interview** selected organizational personnel with media protection responsibilities and **examine** organizational records or documents to determine if the organization consistently applies media labeling on an ongoing basis. **Interview** selected organizational personnel with media protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media labeling control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: MP-4 MEDIA STORAGE		
The organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. The organization protects unmarked media at the highest FIPS 199 security category for the information system until the media are reviewed and appropriately labeled		**Examine** organizational records or documents to determine if the organization protects information system media at the highest FIPS 199 security category for the information system until the media is destroyed or sanitized using approved equipment, techniques, and procedures. **Examine** the location where the organization physically controls and securely stores information system media, both paper and digital, to determine if the organization controls the media at the highest FIPS 199 security category of the information recorded on the media. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media storage control is implemented. **Interview** selected organizational personnel with media protection responsibilities and **examine** organizational records or documents to determine if the organization consistently controls and securely stores information system media on an ongoing basis. **Interview** selected organizational personnel with media protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media storage control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: MP-5 MEDIA TRANSPORT		
		Examine organizational records or documents to determine if the organization restricts the pickup, receipt, transfer, and delivery of information system media (paper and digital) to authorized personnel. **Examine** the list of personnel that have been authorized for the pickup, receipt, transfer, and delivery of information system media to determine if access is appropriately restricted. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media transport control is implemented. **Interview** selected organizational personnel with media protection responsibilities and **examine** organizational records or documents to determine if the organization consistently transports in a secure manner information system media on an ongoing basis. **Interview** selected organizational personnel with media protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media transport control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: MP-6 MEDIA SANITIZATION AND DISPOSAL		
Sanitization is the process used to remove information from information system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, ensure that organizational information is not disclosed to unauthorized individuals when such media is reused or disposed. The organization uses its discretion on sanitization techniques and procedures for media containing information deemed to be in the public domain or deemed to have no adverse impact on the organization if released for reuse or disposed.		**Examine** organizational records or documents to determine if the organization: (i) sanitizes information system media, both paper and digital, using approved equipment, techniques, and procedures prior to disposal or release for reuse; (ii) tracks, documents, and verifies media sanitization actions; and (iii)conducts periodic tests of sanitization equipment to ensure correct performance. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media sanitization and disposal control is implemented. **Interview** selected organizational personnel with media protection responsibilities and **examine** organizational records or documents to determine if the organization consistently applies media sanitization and disposal on an ongoing basis. **Interview** selected organizational personnel with media protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media sanitization and disposal control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Physical And Environmental Protection **Class: Operational**		
Control Number: PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURE		
		Examine organizational records or documents to determine if the physical and environmental protection policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. **Examine** the physical and environmental protection policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. **Examine** the physical and environmental protection procedures to determine if the procedures are sufficient to address all areas identified in the physical and environmental protection policy and all associated physical and environmental protection controls. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the physical and environmental protection policy and procedures control is implemented. **Examine** the physical and environmental protection policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies regulations, standards, and guidance. **Interview** selected organizational personnel with physical and environmental protection responsibilities and **examine** organizational records or documents to determine if the organization consistently applies the physical and environmental protection policy and procedures on an ongoing basis. **Interview** selected organizational personnel with physical and environmental protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the physical and environmental protection policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: PE-2 PHYSICAL ACCESS AUTHORIZATIONS		
The organization promptly removes personnel no longer requiring access from access lists.		**Examine** organizational records or documents to determine if: (i) the organization develops and keeps current a list of personnel with authorized access to the facility containing the information system; (ii) the organization issues appropriate authorization credentials (e.g., badges, identification cards, smart cards); and (iii) designated officials within the organization review and approve the access list and authorization credentials on an organization-defined frequency. **Examine** the facility access list to determine if: (i) the individuals on the list are current personnel assigned to the organization; and (ii) the authorization credentials of the personnel are appropriate.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: PE-2 PHYSICAL ACCESS AUTHORIZATIONS		
		Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the physical access authorizations control is implemented. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records or documents to determine if the organization manages physical access authorizations for the facility on an ongoing basis. **Interview** selected organizational personnel with physical and environmental protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the physical access authorizations control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: PE-3 PHYSICAL ACCESS CONTROL		
The organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems. The organization secures keys, combinations, and other access devices and inventories those devices regularly. The organization changes combinations and keys: (i) periodically; and (ii) when keys are lost, combinations are compromised, or individuals are transferred or terminated. After an emergency-related event, the organization restricts reentry to facilities to authorized individuals only.		**Examine** organizational records or documents and the facility that contains the information system to determine if the organization: (i) controls all physical access points to the facility; (ii) verifies individual access authorizations before granting access to the facility; and (iii) controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk. **Examine** organizational records or documents and selected physical access devices to determine if; (i) physical access devices (e.g., keys, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a regular and scheduled basis; (ii) the organization secures keys, combinations and other access devices on a regular basis; and (iii) keys and combinations to locks within the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are transferred or terminated..

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: PE-3 PHYSICAL ACCESS CONTROL		
Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being appropriately controlled.		
Control Number: PE-6 MONITORING PHYSICAL ACCESS		
The organization reviews physical access logs periodically, investigates apparent security violations or suspicious physical access activities, and takes remedial actions.	(1) The organization monitors real-time intrusion alarms and surveillance equipment. (2) The organization employs automated mechanisms to ensure potential intrusions are recognized and appropriate response actions initiated.	**Examine** organizational records, documents, and the facility where the information system resides to determine if the organization monitors physical access to information systems to detect and respond to incidents. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities to determine how individuals respond to physical access incidents. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the monitoring physical access control is implemented. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records, documents, and the facility where the information system resides to determine if the organization consistently monitors physical access to the system to detect and respond to incidents on an ongoing basis. **Interview** selected organizational personnel with physical and environmental protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the monitoring physical access control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities to determine if real-time intrusion alarms and surveillance equipment are used. **Examine** intrusion alarms and surveillance equipment to determine if the equipment is operational and functioning properly. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities to determine if the organization employs automated mechanisms to recognize potential intrusions and initiate appropriate responses. **Examine** organizational documents or records to determine if physical access intrusions are recognized and appropriate actions initiated. **Test** the automated mechanisms to determine if each automated function is properly configured to recognize potential intrusions and initiate appropriate responses.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: PE-7 VISITOR CONTROL		
	(1) The organization escorts visitors and monitors visitor activity, when required.	**Examine** organizational records, documents, and the facility where the information system resides to determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility or areas other than areas designated as publicly accessible. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the visitor control is implemented. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records, documents, and the facility where the information system resides to determine if the organization controls visitor access to the facility on an ongoing basis. **Interview** selected organizational personnel with physical and environmental protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the visitor control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records, documents, and the facility where the information system resides to determine if the organization escorts visitors and monitors visitor activity, when required.
Control Number: PE-8 ACCESS LOGS		
	(1) The organization employs automated mechanisms to facilitate the maintenance and review of access logs.	**Examine** organizational records or documents to determine if the organization maintains a visitor access log to the facility where the information system resides 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; (vii) name and organization of person visited; and (viii) an indication of a designated official's review of the access log within the organization-defined frequency. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access logs control is implemented. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records or documents to determine if the organization consistently maintains and reviews visitor access logs on an ongoing basis. **Interview** selected organizational personnel with physical and environmental protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access logs control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: PE-8 ACCESS LOGS		
		Interview selected organizational personnel with physical and/or environmental protection responsibilities to determine what automated mechanisms and automated functions are employed to facilitate the maintenance and review of visitor access logs. **Examine** the automated mechanisms within the facility to determine if each automated function is properly configured to ensure that maintenance and review of visitor access logs are properly performed.
Control Number: PE-9 POWER EQUIPMENT AND POWER		
	(1) The organization employs redundant and parallel power cabling paths	**Examine** organizational records, documents, and the facility where the information system resides to determine if the organization protects power equipment and power cabling for the information system from damage and destruction. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the power equipment and power cabling control is implemented. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records or documents to determine if the organization consistently protects power equipment and power cabling for the information system on an ongoing basis. **Interview** selected organizational personnel with physical and environmental protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the power equipment and power cabling control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine**e organizational records, documents, and the facility where the information system resides to determine if the organization employs redundant and parallel power cabling paths.
Control Number: PE-10 EMERGENCY SHUTOFF		
		Interview selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records, documents, and the facility containing concentrations of information system resources to determine if the organization provides the capability of shutting off power to any information system component that may be malfunctioning or threatened. **Examine** the emergency shutoff capability to ensure that it exists and is functional. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the emergency shutoff control is implemented.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: PE-10 EMERGENCY SHUTOFF		
		Interview selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records, documents, and the facility containing concentrations of information system resources to determine if the organization consistently employs an emergency shutoff capability for the information system on an ongoing basis. **Interview** selected organizational personnel with physical and environmental protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the emergency shutoff control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: PE-11 EMERGENCY POWER		
	(1) The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source. (2) The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.	**Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records, documents, and the facility where the information system resides to determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the system in the event of a primary power source loss. **Examine** organizational records or documents to determine if the results of the last tested power outage demonstrated the availability of a short-term power supply for the information system. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the emergency power control is implemented. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records, documents, and the facility where the information system resides to determine if the organization consistently provides an emergency power capability for the information system on an ongoing basis. **Interview** selected organizational personnel with physical and environmental protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the emergency power control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records or documents to determine if the organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: PE-11 EMERGENCY POWER		
		Examine organizational records or documents to determine if the results of the last tested power outage demonstrated the availability of a long-term alternate power supply for the information system. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records or documents to determine if the organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation. **Examine** organizational records or documents to determine if the results of the last tested power outage demonstrated the availability of a long-term, self-contained alternate power supply for the information system.
Control Number: PE-12 EMERGENCY LIGHTING		
		Interview selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records, documents, and the facility where the information system resides to determine if the organization employs and maintains an automatic emergency lighting system that activate in the event of a power outage or disruption and that covers emergency exits and evacuation routes. **Examine** organizational records or documents to determine if the results of the last tested power outage demonstrated that the emergency lighting system was operational and fully functional. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the emergency lighting control is implemented. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records or documents to determine if the organization provides and maintains an emergency lighting system for the information system on an ongoing basis. **Interview** selected organizational personnel with physical and environmental protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the emergency lighting control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: PE-13 FIRE PROTECTION		
Fire suppression and detection devices/systems include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.	(1) Fire suppression and detection devices/systems activate automatically in the event of a fire.	**Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records, documents, and the facility where the information system resides to determine if the organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire. **Examine** the results of the last test of the fire suppression and detection devices/systems to determine if the fire protection resources can be successfully activated in the event of a fire.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: PE-13 FIRE PROTECTION		
	(2) Fire suppression and detection devices/systems provide automatic notification of any activation to the organization and emergency responders.	**Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the fire protection control is implemented. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records or documents to determine if the organization consistently provides fire suppression and detection devices/systems for the facility where the information system resides on an ongoing basis. **Interview** selected organizational personnel with physical and environmental protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the fire protection control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records or documents to determine if fire suppression and detection devices/systems activate automatically in the event of a fire. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities to determine if the fire suppression and detection devices/systems for the facility where the information system resides provide automatic notification of any activation to the organization and emergency responders. **Examine** the alarm system service level agreement to determine if the agreement details automatic notification to the organization and emergency responders. **Examine** organizational records or documents to determine if the results of the last test of the fire suppression and detection devices/systems demonstrated that the organization and emergency responders were automatically notified.
Control Number: PE-14 TEMPERATURE AND HUMIDITY CONTROLS		
		Interview selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records or documents to determine if the organization regularly maintains, within acceptable levels, and monitors the temperature and humidity of the facility where the information system resides. **Examine** the facility where the information system resides to determine if the temperature and humidity controlling systems are in place and functioning as intended. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the temperature and humidity control is implemented. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records or documents to determine if the organization consistently maintains and monitors temperature and humidity levels within the facility where the information system resides on an ongoing basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: PE-14 TEMPERATURE AND HUMIDITY CONTROLS		
		Interview selected organizational personnel with physical and environmental protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the temperature and humidity control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: PE-15 WATER DAMAGE PROTECTION		
	(1) The organization employs automated mechanisms to automatically close shutoff valves in the event of a significant water leak.	**Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records or documents to determine if the organization protects the information system from water damage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel. **Examine** the facility where the information system resides to determine if the master shutoff valves are accessible and working properly. **Examine** organizational records or documents to determine if the results of the last test of the environmental controls of the facility where the information system resides demonstrate that the master shutoff valves are working properly. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the water damage protection control is implemented. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records or documents to determine if the organization consistently protects the information system from water damage on an ongoing basis. **Interview** selected organizational personnel with physical and environmental protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the water damage protection control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities to determine if automated mechanisms and automated functions are employed to automatically close shutoff valves in the event of a significant water leak. **Examine** the automated mechanisms for water shutoff valves within the facility to determine if each automated function is properly configured to ensure that water valves can be automatically shut off in the event of a significant water leak.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: PE-16 DELIVERY AND REMOVAL		
The organization controls delivery areas and, if possible, isolates the areas from the information system and media libraries to avoid unauthorized access. Appropriate organizational officials authorize the delivery or removal of information system-related items belonging to the organization.		**Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records or documents to determine if the organization controls the information system-related items (i.e., hardware, firmware, software) entering and exiting the facility where the system resides and maintains appropriate records of those items. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the delivery and removal control is implemented. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records or documents to determine if the organization consistently controls the delivery and removal of information system-related items from the facility where the system resides on an ongoing basis. **Interview** selected organizational personnel with physical and environmental protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the delivery and removal control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: PE-17 ALTERNATE WORK SITE		
		Interview selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records or documents to determine if individuals within the organization employ appropriate information system security controls at alternate work sites. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the alternate work site control is implemented. **Examine** the alternate work sites to determine if appropriate information system security controls are in place. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records, documents, and alternate work sites to determine if individuals within the organization consistently employ appropriate information system security controls at alternate work sites on an ongoing basis. **Interview** selected organizational personnel with physical and environmental protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the alternate work site control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS		
Physical and environmental hazards include, for example, flooding, vandalism, electrical interference, electromagnetic radiation, eating and drinking within proximity.		**Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records or documents to determine if the organization positions information system components within the facility to minimize potential damage from environmental hazards (e.g., electrical interference, electromagnetic radiation, vandalism, eating, drinking, smoking in the proximity, information leakage due to emanation) and to minimize the opportunity for unauthorized access. **Examine** the facility where the information system components reside to determine if the organization positions components to minimize potential damage from environmental hazards and to minimize the opportunity for unauthorized access. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the location of information system components control is implemented. **Interview** selected organizational personnel with physical and/or environmental protection responsibilities and **examine** organizational records, documents, and the facility where the information system resides to determine if the organization consistently manages the location of system components to minimize risk on an ongoing basis. **Interview** selected organizational personnel with physical and environmental protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the location of information system components control are documented and the resulting information used to actively improve the control on a continuous basis.
Security Planning **Class: Management**		
Control Number: PL-1 SECURITY PLANNING POLICY AND PROCEDURES		
		Examine organizational records or documents to determine if security planning policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. **Examine** the security planning policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. **Examine** the security planning procedures to determine if the procedures are sufficient to address all areas identified in the security planning policy and all associated security planning controls.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: PL-1 SECURITY PLANNING POLICY AND PROCEDURES		
		Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security planning policy and procedures control is implemented. **Examine** the security planning policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies regulations, standards, and guidance. **Interview** selected organizational personnel with security planning and plan implementation responsibilities and **examine** organizational records or documents to determine if the organization consistently applies the security planning policy and procedures on an ongoing basis. **Interview** selected organizational personnel with security planning and plan implementation responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security planning policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: PL-2 SYSTEM SECURITY PLAN		
		Examine organizational records or documents to determine if the security plan: (i) exists; (ii) is documented; (iii) is disseminated to appropriate elements within the organization; and (iv) is reviewed and approved by responsible officials within the organization. **Examine** the security plan to determine if the plan is consistent with NIST Special Publication 800-18 and addresses security roles, responsibilities, assigned individuals with contact information, and activities for planning security of the information system. **Interview** selected organizational personnel with security planning and plan implementation responsibilities to determine if key operating elements within the organization understand the security plan and are ready to implement the plan. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system security plan control is implemented. **Interview** selected organizational personnel with security planning and plan implementation responsibilities and **examine** organizational records or documents to determine if organizational officials consistently review and approve the security plan for the information system on an ongoing basis. **Interview** selected organizational personnel with security planning and plan implementation responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the system security plan control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: PL-3 SYSTEM SECURITY PLAN UPDATE		
Significant changes are defined in advance by the organization and identified in the configuration management process.		**Examine** organizational records or documents to determine if the security plan is updated in accordance with organization-defined frequency. **Examine** the security plan to determine if the revised plan reflects the needed changes based on the organization's experiences during plan implementation. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system security plan update control is implemented. **Interview** selected organizational personnel with security planning and plan implementation responsibilities and **examine** organizational records or documents to determine if the organization consistently reviews and updates the security plan for the information system on an ongoing basis. **Interview** selected organizational personnel with security planning and plan implementation responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security plan update control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: PL-4 RULES OF BEHAVIOR		
Electronic signatures are acceptable for use in acknowledging rules of behavior. NIST Special Publication 800-18 provides guidance on preparing rules of behavior.		**Examine** organizational records or documents to determine if the organization provides and makes readily available to all information system users a set of rules that describes users' responsibilities and expected behavior with regard to information and information system usage. **Examine** organizational records or documents to determine if the organization receives a 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. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the rules of behavior control is implemented. **Interview** selected organizational personnel with security planning and plan implementation responsibilities and **examine** organizational records or documents to determine if the organization consistently reviews and updates the rules of behavior on an ongoing basis. **Interview** selected organizational personnel with security planning and plan implementation responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the rules of behavior control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: PL-5 PRIVACY IMPACT ASSESSMENT		
		Examine organizational records or documents to determine if the organization conducts a privacy impact assessment on the information system. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the privacy impact assessment control is implemented. **Interview** selected organizational personnel with security planning and plan implementation responsibilities and **examine** organizational records or documents to determine if the organization consistently conducts privacy impact assessments on the information system on an ongoing basis. **Interview** selected organizational personnel with security planning and plan implementation responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the privacy impact assessment control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: PL-6 SECURITY-RELATED ACTIVITY PLANNING		
Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises.		**Examine** organizational records or documents to determine if appropriate planning and coordination occur before conducting security-related activities affecting the information system. **Interview** selected organizational personnel with security planning and plan implementation responsibilities to determine if key operating elements within the organization understand the breath and depth of ongoing security-related activities in order to minimize the impact on organizational operations (i.e., mission, functions, image, and reputation) and organizational assets. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security-related activity planning control is implemented. **Interview** selected organizational personnel with security planning and plan implementation responsibilities and **examine** organizational records or documents to determine if the organization consistently plans and coordinates with appropriate organizational elements prior to initiating security-related activities on an ongoing basis. **Interview** selected organizational personnel with security planning and plan implementation responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security-related activity planning control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Personnel Security **Class: Operational**		
Control Number: PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES		
The personnel security policy and procedures are consistent with applicable RT Standards.		**Examine** organizational records or documents to determine if the personnel security policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. **Examine** the personnel security policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. **Examine** the personnel security procedures to determine if the procedures are sufficient to address all areas identified in the personnel security policy and all associated personnel security controls. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel security policy and procedures control is implemented. **Examine** the personnel security policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies regulations, standards, and guidance. **Interview** selected organizational personnel with personnel security responsibilities and **examine** organizational records or documents to determine if the organization consistently applies the personnel security policy and procedures on an ongoing basis. **Interview** selected organizational personnel with personnel security responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personnel security policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: PS-2 POSITION CATEGORIZATION		
		Examine the organizational records or documents to determine if the organization: (i) establishes risk designations; (ii) assigns a risk designation to all organizational positions; (iii) follows screening criteria for individuals filling organizational positions; and (iv) reviews and revises position risk designations on an organization-defined frequency. **Test** the position categorization procedures by comparing a list of organizational personnel and their clearance and/or authorization levels to the position risk designations to determine if the organization meets the screening criteria for those individuals filling the positions.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: PS-3 PERSONNEL SCREENING		
Screening is consistent with the RT Standards.		**Examine** organizational records or documents to determine if the organization appropriately screens individuals requiring access to organizational information and information systems prior to authorizing access. **Test** the personnel screening process by comparing a list of organizational personnel requiring access to the information system and their associated screening dates to account creation dates to determine if the organization meets the screening criteria for those individuals. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel screening control is implemented. **Interview** selected organizational personnel with personnel security responsibilities and **examine** organizational records or documents to determine if the organization consistently conducts personnel screening for positions within the organization on an ongoing basis. **Interview** selected organizational personnel with personnel security responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personnel screening control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: PS-4 PERSONNEL TERMINATION		
		Examine organizational records or documents to determine if the organization: (i) revokes the information system accounts of terminated personnel; (ii) conducts exit interviews of terminated personnel; (iii) collects all information system-related property (e.g., keys, identification cards, building passes) of terminated personnel; and (iv) retains access to official documents and records on organizational information systems created by terminated personnel. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel termination control is implemented.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: PS-4 PERSONNEL TERMINATION		
		Interview selected organizational personnel with personnel security responsibilities and **examine** organizational records or documents to determine if the organization consistently manages personnel termination activities to protect organizational operations and assets on an ongoing basis. **Interview** selected organizational personnel with personnel security responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personnel termination control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: PS-5 PERSONNEL TRANSFER		
		Examine organizational records or documents to determine if the organization: (i) reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization; and (ii) initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorization) for personnel reassigned or transferred within the organization. **Test** the personnel transfer procedures of the organization by comparing the information system authorizations of current personnel to the access authorizations of transferred personnel to determine if all personnel have appropriate authorizations for the information system. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel transfer control is implemented. **Interview** selected organizational personnel with personnel security responsibilities and **examine** organizational records or documents to determine if the organization consistently manages personnel transfer activities to protect organizational operations and assets on an ongoing basis. **Interview** selected organizational personnel with personnel security responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personnel transfer control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: PS-6 ACCESS AGREEMENTS		
		Examine organizational records or documents to determine if the organization: (i) 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; and (ii) reviews and updates the access agreements on an organization-defined frequency.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: PS-6 ACCESS AGREEMENTS		
		Examine selected access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for the information system to determine if the access agreements are: (i) signed and retained in accordance with the documented organizational policy and procedures; and (ii) reviewed and updated by the organization on an organization-defined frequency. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access agreements control is implemented. **Interview** selected organizational personnel with personnel security responsibilities and **examine** organizational records or documents to determine if the organization consistently completes, reviews, and updates access agreements on an ongoing basis. **Interview** selected organizational personnel with personnel security responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access agreements control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: PS-7 THIRD-PARTY PERSONNEL SECURITY		
The organization explicitly includes personnel security requirements in acquisition-related documents in accordance with the RT Standards.		**Examine** organizational records or documents to determine if the organization:(i) establishes personnel security requirements, including security roles and responsibilities, 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 (ii) monitors third-party provider compliance to ensure adequate security. **Interview** selected organizational personnel with personnel security responsibilities to determine if the organization monitors third-party provider compliance with personnel security requirements. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the third-party personnel security control is implemented. **Interview** selected organizational personnel with personnel security responsibilities and **examine** organizational records or documents to determine if the organization consistently establishes and monitors personnel security requirements for third-party providers on an ongoing basis. **Interview** selected organizational personnel with personnel security responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the third-party personnel security control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: PS-8 PERSONNEL SANCTIONS		
The sanctions process can be included as part of the general personnel policies and procedures for the organization.		**Examine** organizational records or documents to determine if the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures. **Examine** organizational records or documents including signed rules of behavior to determine if the organization defines and conveys the formal sanctions process to organizational personnel. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel sanctions control is implemented. **Interview** selected organizational personnel with personnel security responsibilities and **examine** organizational records or documents to determine if the organization consistently employs and monitors personnel sanctions on an ongoing basis. **Interview** selected organizational personnel with personnel security responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personnel sanctions control are documented and the resulting information used to actively improve the control on a continuous basis.
Risk Assessment **Class: Management**		
Control Number: RA-1 RISK ASSESSMENT POLICY AND PROCEDURES		
		Examine organizational records or documents to determine if risk assessment policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. **Examine** the risk assessment policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. **Examine** the risk assessment procedures to determine if the procedures are sufficient to address all areas identified in the risk assessment policy and all associated risk assessment controls.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: RA-1 RISK ASSESSMENT POLICY AND PROCEDURES		
		Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the risk assessment policy and procedures control is implemented. **Examine** the risk assessment policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies, regulations, standards, and guidance. **Interview** selected organizational personnel with risk assessment responsibilities and **examine** organizational records or documents to determine if the organization consistently applies the risk assessment policy and procedures on an ongoing basis. **Interview** selected organizational personnel with risk assessment responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the risk assessment policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: RA-2 SECURITY CATEGORIZATION		
NIST Special Publication 800-60 provides guidance on determining the security categories of the information types resident on the information system. The organization conducts security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, information system owners, and information owners.		**Examine** the system security plan to determine if the security categorization of the information system: (i) exists; (ii) is consistent with FIPS 199; (iii) includes supporting rationale consistent with NIST Special Publication 800-60; and (iv) is reviewed and approved by designated senior-level officials within the organization. **Interview** selected organizational personnel with risk assessment responsibilities to determine if the security categorization process is conducted as an organization-wide exercise with the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and information owners. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security categorization control is implemented. **Interview** selected organizational personnel with risk assessment responsibilities and **examine** organizational records or documents to determine if the organization consistently conducts security categorizations of the information system on an ongoing basis. **Interview** selected organizational personnel with risk assessment responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security categorization control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: RA-3 RISK ASSESSMENT		
Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., Service Providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities).		**Examine** organizational records or documents to determine if the organization assesses 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 its operations and assets (including information and information systems managed/operated by external parties). **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the risk assessment control is implemented. **Interview** selected organizational personnel with risk assessment responsibilities and **examine** organizational records or documents to determine if the organization consistently conducts risk assessments for the information system on an ongoing basis. **Interview** selected organizational personnel with personnel security responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the risk assessment control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: RA-4 RISK ASSESSMENT UPDATE		
The organization develops and documents specific criteria for what is considered significant change to the information system.		**Examine** organizational records or documents to determine if the risk assessment is updated in accordance with 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. **Examine** the risk assessment to determine if the report reflects the latest significant changes to the information system, the facilities where the system resides, or other conditions that may have impacted the security or accreditation status of the system. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the risk assessment update control is implemented. **Interview** selected organizational personnel with risk assessment responsibilities and **examine** organizational records or documents to determine if the organization consistently reviews and updates the risk assessment for the information system on an ongoing basis. **Interview** selected organizational personnel with risk assessment responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the risk assessment update control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: RA-5 VULNERABILITY SCANNING		
Vulnerability scanning is conducted using appropriate scanning tools and techniques. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk.	(1) Vulnerability scanning tools include the capability to readily update the list of information system vulnerabilities scanned. (2) The organization updates the list of information system vulnerabilities scanned [Assignment: organization-defined frequency] or when significant new vulnerabilities are identified and reported.	**Examine** organizational records or documents to determine if the organization scans for vulnerabilities in the information system on an organization-defined frequency or when significant new vulnerabilities affecting the system are identified and reported. **Examine** the latest vulnerability scanning results to determine if the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the vulnerability scanning control is implemented. **Interview** selected organizational personnel with risk assessment responsibilities and **examine** organizational records or documents to determine if the organization consistently conducts vulnerability scanning of the information system on an ongoing basis. **Interview** selected organizational personnel with risk assessment responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the vulnerability scanning control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: RA-5 VULNERABILITY SCANNING		
The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code).	(3) Vulnerability scanning procedures include means to ensure adequate scan coverage, both vulnerabilities checked and information system components scanned.	**Interview** selected organizational personnel with risk assessment responsibilities to determine if the organization uses vulnerability scanning tools that have the capability to readily update the list of information system vulnerabilities scanned. **Examine** previous vulnerability scan results to ensure that the tools used for vulnerability scanning include the capability to update the list of information system vulnerabilities scanned. **Examine** organizational records or documents to determine if the organization updates the list of information system vulnerabilities scanned on an organization-defined frequency or when significant new vulnerabilities are identified and reported. **Examine** organizational records or documents to determine if the organization provides adequate vulnerability scanning coverage including the key components of the information system (as defined by the organization) and the most up-to-date vulnerabilities. PAGE 201
System And Services Acquisition **Class: Management**		
Control Number: SA-5 INFORMATION SYSTEM DOCUMENTATION		
Administrator and user guides include information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features.	(1) The organization includes 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. (2) The organization includes documentation,	**Examine** organizational records or documents to determine if the organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel. **Examine** organizational records or documents to ensure that administrator and user guides include information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system documentation control is implemented. **Interview** selected organizational personnel with system and services acquisition responsibilities and **examine** organizational records or documents to determine if the organization consistently provides, protects, and distributes information system documentation on an ongoing basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SA-5 INFORMATION SYSTEM DOCUMENTATION		
	if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).	**Interview** selected organizational personnel with system and services acquisition responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system documentation control are documented and the resulting information used to actively improve the control on a continuous basis. **Examine** organizational records or documents to determine if the information system documentation describes the functional properties of the security controls employed within the system with sufficient detail to permit analysis and testing of the controls. **Examine** organizational records or documents to determine if the information system documentation describes the design and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).
Control Number: SA-6 SOFTWARE USAGE RESTRICTIONS		
Software and associated documentation are used in accordance with contract agreements and copyright laws. For software and associated documentation protected by quantity licenses, the organization employs tracking systems to control copying and distribution. The organization controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.		**Examine** organizational records or documents to determine if the organization regularly reviews/analyzes software usage for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the software usage restrictions control is implemented. **Interview** selected organizational personnel with system and services acquisition responsibilities and **examine** organizational records or documents to determine if the organization consistently enforces software usage restrictions on an ongoing basis. **Interview** selected organizational personnel with system and services acquisition responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the software usage restrictions control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SA-7 USER INSTALLED SOFTWARE		
		Examine organizational documents or records to determine if the organization enforces explicit rules regarding the downloading and installation of software by users. **Examine** organizational documents or records to determine if the organization regularly reviews/analyzes user installed software for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. **Examine** firewall logs for indications that prohibited software is operational within the information system. (Note: applications tend to communicate on known ports and/or have signature traffic patterns and common packets.) **Test** the enforcement of rules for user installed software on the information system by attempting to download and install (from an account with user privileges) software that is strictly prohibited; compare the results with a similar test conducted on an account with administrative privileges; determine which account rights violated the rules for user installed software. **Test** network traffic on the information system to determine if prohibited software is installed and operational by utilizing a network packet analyzer. (Note: Applications tend to communicate on known ports and/or have signature traffic patterns and common packets.) **Test** the information system for prohibited software by utilizing a scanner which detects and reports the names of installed software; compare the results against the approved software applications list. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the user installed software control is implemented. **Interview** selected organizational personnel with system and services acquisition responsibilities and **examine** organizational records or documents to determine if the organization consistently enforces rules for the downloading and installation of software by users on an ongoing basis. **Interview** selected organizational personnel with system and services acquisition responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the user installed software control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: SA-8 SECURITY DESIGN PRINCIPLES		
		Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security design principles control is implemented. **Interview** selected organizational personnel with system and services acquisition responsibilities and **examine** organizational records or documents to determine if the organization consistently applies security design principles in the development and implementation of organizational information systems on an ongoing basis. **Interview** selected organizational personnel with system and services acquisition responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security design principles control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SA-9 OUTSOURCED INFORMATION SYSTEM SERVICES		
Third-party providers are subject to the same information system security policies and procedures of the supported organization, and must conform to the same security control and documentation requirements as would apply to the organization's internal systems. Appropriate organizational officials approve outsourcing of information system services to third-party providers (e.g., service bureaus, contractors, and other external organizations). The outsourced information system services documentation includes Service Provider, and end user security roles and responsibilities, and any service level agreements. Service level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.		**Examine** organizational records or documents to determine if the organization ensures that third-party providers of information system services employ adequate security controls in the information systems providing such services in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. **Examine** organizational records or documents to determine if the organization regularly reviews/analyzes outsourced information system services for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the outsourced information system services control implemented. **Examine** the security control assessment results from the organization providing outsourced information system services to determine if the security controls employed by third-party providers are compliant with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. **Interview** selected organizational personnel with system and services acquisition responsibilities and **examine** organizational records or documents to determine if third-party providers of information system services consistently employ adequate security controls in the information systems providing those services on an ongoing basis. **Interview** selected organizational personnel with system and services acquisition responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the outsourced information system services control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SA-10 DEVELOPER CONFIGURATION MANAGEMENT		
		Examine the information system developer configuration management plan to determine if the developer creates and implements a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and the plan implementation. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the developer configuration management control is implemented. **Interview** selected organizational personnel with system and services acquisition responsibilities and **examine** organizational records or documents to determine if the information system developer consistently manages the information system configuration on an ongoing basis. **Interview** selected organizational personnel with system and services acquisition responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the developer configuration management control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: SA-11 DEVELOPER SECURITY TESTING		
Developmental security test results should only be used when no security relevant modifications of the information system have been made subsequent to developer testing and after selective verification of developer test results.		**Examine** the information system developer's organizational records or documents to determine if the developer creates a security test and evaluation plan, implements the plan, and documents the results. **Examine** organizational records or documents to determine if the organization includes the developer's security test and evaluation results in the organization's Plan of Action and Milestones. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the developer security testing control is implemented. **Interview** selected organizational personnel with system and services acquisition responsibilities and **examine** organizational records or documents to determine if the information system developer consistently implements security testing on an ongoing basis. **Interview** selected organizational personnel with system and services acquisition responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the developer security testing control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
System And Communications Protection **Class: Technical**		
Control Number: SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES		
The system and communications protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required.		**Examine** organizational records or documents to determine if system and communications protection policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. **Examine** the system and communications protection policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. **Examine** the system and communications protection procedures to determine if the procedures are sufficient to address all areas identified in the system and communications protection policy and all associated system and communications protection controls. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system and communications protection policy and procedures control is implemented. **Examine** the system and communications protection policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies regulations, standards, and guidance. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the system and communications protection policy and procedures are consistently applied on an ongoing basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the system and communications protection policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: SC-2 APPLICATION PARTITIONING		
The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management).		**Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system physically and/or logically separates user functionality (including user interface services) from information system management functionality and how the separation is implemented and enforced. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the application partitioning control is implemented.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SC-2 APPLICATION PARTITIONING		
Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.		**Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the information system consistently implements application partitioning on an ongoing basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the application partitioning control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: SC-3 SECURITY FUNCTION ISOLATION		
The information system isolates security functions from non-security functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.	(1) The information system employs underlying hardware separation mechanisms to facilitate security function isolation. (2) The information system further divides the security functions with the functions enforcing access and information flow control isolated and protected from both non-security functions and from other security functions.	**Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system isolates security functions from non-security functions (including control of access to and integrity of the hardware, software, and firmware that perform those security functions) and how the system implements and enforces the isolation (e.g., partitions, domains, etc.). **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security function isolation control is implemented. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system consistently implements security function isolation on an ongoing basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security function isolation control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system employs hardware separation mechanisms to facilitate security function isolation.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SC-3 SECURITY FUNCTION ISOLATION		
	(3) The information system minimizes the amount of non-security functions included within the isolation boundary containing security functions. (4) The information system security maintains its security functions in largely independent modules that avoid unnecessary interactions between modules. (5) The information system security maintains its security functions in a layered structure minimizing interactions between layers of the design.	**Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system isolates critical security functions (i.e., functions enforcing access and information flow control) from both non-security functions and from other security functions. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system minimizes the number of non-security functions included within the isolation boundary containing security functions **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system maintains its security functions in largely independent modules that avoid unnecessary interactions between modules. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system security maintains its security functions in a layered structure minimizing interactions between layers of the design.
Control Number: SC-4 INFORMATION REMNANTS		
Control of information system remnants, sometimes referred to as object reuse, prevents information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains		**Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system prevents unauthorized and unintended information transfer via shared system resources and how the system prevents the transfer. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information remnants control is implemented. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system employs appropriate mechanisms to consistently prevent unauthorized and unintended transfer of information via shared system resources on an ongoing basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SC-4 INFORMATION REMNANTS		
access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.		**Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information remnants control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: SC-5 DENIAL OF SERVICE PROTECTION		
A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, network perimeter devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy.	(1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks. (2) The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.	**Examine** organizational records or documents (including developer design documentation) to determine if the information system protects against or limits the effects of the organization-defined types of denial of service attacks. **Examine** organizational records or documents to determine if the organization uses automated tools to protect against or limit the effects of organization-defined types of denial of service attacks. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the denial of service protection control is implemented. **Test** the denial of service protection by simulating the launching of known denial of service/distributed denial of service attacks with automated tools (e.g. ping of death, teardrop, trinoo). **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the organization consistently implements denial of service protection for the information system on an ongoing basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the denial of service protection control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system restricts the ability of users to launch denial of service attacks against other information systems or networks. **Test** the denial of service protection for the information system by simulating the launching of known denial of service/distributed denial of service attacks with automated tools (e.g. ping of death, teardrop, trinoo). **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system limits the effects of information flooding types of denial of service attacks. **Test** the denial of service protection for the information system by simulating the launching of known denial of service/distributed denial of service attacks with automated tools (e.g. ping of death, teardrop, trinoo).

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SC-6 RESOURCE PRIORITY		
Priority protection ensures that a lower-priority process is not able to interfere with the information system servicing any higher-priority process.		**Examine** organizational records or documents (including developer design documentation) to determine if information system resources have been prioritized and how the system limits the use of resources by priority. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that resource priority control is implemented. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the information system consistently limits the use of resources by priority on an ongoing basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the resource priority control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: SC-7 BOUNDARY PROTECTION		
	(1) The organization physically allocates publicly accessible information system components (e.g., public web servers) to separate sub-networks with separate, physical network interfaces. The organization prevents public access into the organization's internal networks except as appropriately mediated.	**Examine** organizational records or documents (including developer design documentation) to determine if the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the boundary protection control is implemented. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the organization protects the boundaries of the information system using appropriate tools, techniques, and technologies on an ongoing basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the boundary protection control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if: (i) the organization physically allocates publicly accessible information system components (e.g., public web servers) to separate sub-networks with separate, physical network interfaces; and (ii) the organization prevents public access into the organization's internal networks except as appropriately mediated.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SC-8 TRANSMISSION INTEGRITY		
	(1) The organization employs cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).	**Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system protects the integrity of transmitted information and how the integrity protections are implemented (i.e., mechanisms, tools, techniques, and technologies). **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that transmission integrity control is implemented. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the information system consistently protects the integrity of transmitted information on an ongoing basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the transmission integrity control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the organization employs cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems). **Examine** organizational records or documents (including developer design documentation) to determine how the organization employs cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems). **Test** the cryptographic mechanisms employed in the information system used to achieve transmission integrity by attempting to exploit any known vulnerabilities.
Control Number: SC-9 TRANSMISSION CONFIDENTIALITY		
	(1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).	**Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system protects the confidentiality of transmitted information and how the confidentiality protections are implemented (i.e., mechanisms, tools, techniques, and technologies). **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the transmission confidentiality control is implemented. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the information system consistently protects the confidentiality of transmitted information on an ongoing basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SC-9 TRANSMISSION CONFIDENTIALITY		
		Interview selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the transmission confidentiality control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems). **Examine** organizational records or documents (including developer design documentation) to determine how the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems). **Test** the cryptographic mechanisms employed in the information system used to achieve transmission confidentiality by attempting to exploit any known vulnerabilities.
Control Number: SC-10 NETWORK DISCONNECT		
		Interview selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system terminates a network connection at the end of a session or after an organization-defined time period of inactivity and how the connection is terminated. **Test** the network disconnection capability for the information system by leaving an open session for a specified amount of time to determine if the system terminates the network connection as expected. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the network disconnect control is implemented. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system consistently terminates network connections after an organization-defined period of inactivity on an ongoing basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the network disconnect control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SC-11 TRUSTED PATH		
		Interview selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system establishes a trusted communications path between the user and the security functionality of the system and how the trusted path is implemented. **Test** the information system trusted path by attempting to establish both a trusted and non-trusted communication path between the user and the security functionality of the system. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the trusted path control is implemented. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the information system consistently implements a trusted communications path on an ongoing basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the trusted path control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT		
		Interview selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and management and how the mechanisms and procedures are implemented. **Test** the information system cryptographic key establishment and management by using the automated mechanisms to walk a test key through all the phases of its lifecycle from generation to revocation. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the cryptographic key establishment and management control is implemented. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the information system consistently employs automated mechanisms with supporting procedures or the organization employs manual procedures for cryptographic key establishment and management on an ongoing basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the cryptographic key establishment and management control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SC-13 USE OF VALIDATED CRYPTOGRAPHY		
		Examine organizational records or documents (including developer design documentation) to determine if the employed cryptography complies with encryption standards in the RT Standards and RTIC Technical Interoperability Specification. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the use of validated cryptography control is implemented. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the organization consistently uses validated cryptography within the information system on an ongoing basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the use of validated cryptography control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: SC-14 PUBLIC ACCESS PROTECTIONS		
		Interview selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if, for publicly available information systems, the system protects the integrity of the information and applications and how the protections are implemented. **Test** the publicly available information system by attempting to alter protected information using a public account to determine if access is limited in order to preserve the integrity of the information and the applications. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the public access protections control is implemented. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the information system consistently protects the integrity of the information and applications on public access systems on an ongoing basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the public access protections control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SC-15 COLLABORATIVE COMPUTING		
	(1) The information system provides physical disconnect of camera and microphone in a manner that supports ease of use.	**Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if 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) and how remote activation of collaborative computing is prohibited. **Test** the information system by attempting to remotely control video or audio capabilities to determine if remote activation of collaborative computing mechanisms is restricted. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the collaborative computing control is implemented. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the information systems consistently implements restrictions on the use of collaborative computing on an ongoing basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the collaborative computing control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the information system provides physical disconnect of cameras and microphones in a manner that supports ease of use and how the information system provides physical disconnect of these components.
Control Number: SC-16 TRANSMISSION OF SECURITY PARAMETERS		
Security parameters may be explicitly or implicitly associated with the information contained within the information system.		**Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system associates security parameters (e.g., security labels and markings) with information exchanged between information systems and how the transmission of security parameters is implemented. **Test** the information system's ability to associate security parameters between information systems by exchanging data between systems at different sensitivity levels. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the transmission of security parameters control is implemented. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the information system consistently transmits security parameters reliably between information systems on an ongoing basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SC-16 TRANSMISSION OF SECURITY PARAMETERS		
		Interview selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the transmission of security parameters control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: SC-18 MOBILE CODE		
Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the information system.		**Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if 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; (ii) documents, monitors, and controls the use of mobile code within the information system; and (iii) requires organizational officials to approve the use of mobile code. **Test** the information system by attempting to run mobile code in an application where it is specifically prohibited to determine if the organization implements mobile code usage restrictions. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the mobile code control is implemented. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if mobile code is consistently restricted on an ongoing basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the mobile code control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: SC-19 VOICE OVER INTERNET PROTOCOL		
		Interview selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the organization: (i) establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously; (ii) documents, monitors, and controls the use of VoIP within the information system; and (iii) requires organizational officials to approve the use of VoIP. **Test** the VoIP capability by attempting to spoof or mask a caller's identity. **Test** the VoIP capability by attempting to generate enough network volume to create a denial of service attack.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SC-19 VOICE OVER INTERNET PROTOCOL		
		Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the VoIP control is implemented. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the organization consistently manages VoIP technology by establishing usage restrictions and monitoring, documenting, and controlling the use of the technology within the information on an ongoing basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the VoIP control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: SC-19 SECURE NAME LOOKUP SERVICE (AUTHORITATIVE SOURCE)		
	(1) The information system verifies the authenticity of the artifacts for data origin authentication and data integrity (i.e., public key) of any subsidiary (child) zone in the name space in instances where the subsidiary (child) zone possesses this capability (i.e., provides these artifacts).	**Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system (i.e., authoritative domain name servers) that provides the name lookup service for accessing organizational information resources to entities across the Internet provides artifacts for data origin authentication and data integrity to enable users to obtain message authentication and message integrity assurances for the information received during network-based transactions and how the information system provides artifacts for data origin authentication and data integrity. **Test** the information system by attempting to launch known attacks against the domain name servers. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the secure name lookup service (authoritative source) control is implemented. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the secure name lookup service (authoritative source) is consistently implemented on an ongoing basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the secure name lookup service (authoritative source) control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SC-19 SECURE NAME LOOKUP SERVICE (AUTHORITATIVE SOURCE)		
		Interview selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the information system verifies the authenticity of the artifacts for data origin authentication and data integrity (i.e., public key) of any subsidiary (child) zone in the name space in instances where the subsidiary (child) zone possesses this capability (i.e., provides these artifacts) and how the information system verifies the authenticity of the artifacts for data origin authentication and data integrity.
Control Number: SC-21 SECURE NAME LOOKUP SERVICE (RESOLUTION)		
	(1) The information system performs data origin authentication and data integrity verification for all information received whether or not client systems issue such requests.	**Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents (including developer design documentation) to determine if the information system (i.e., authoritative domain name servers) that provides the name lookup service for accessing information resources to entities within the organization provides mechanisms for data origin authentication and data integrity verification and performs these services when requested by client systems and how the information system provides mechanisms for data origin authentication and data integrity verification. **Test** the information system by attempting to launch known attacks against the domain name servers. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the secure name lookup service (resolution) control is implemented. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the secure name lookup service (resolution) is consistently implemented on an ongoing basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the secure name lookup service (resolution) control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with system and communications protection responsibilities and **examine** organizational records or documents to determine if the information system performs data origin authentication and data integrity verification for all information received whether or not client systems issue such requests and how the information system performs data origin authentication and data integrity verification.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
System and Information Integrity **Class: Operational**		
Control Number: SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES		
The system and information integrity policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required.		**Examine** organizational records or documents to determine if system and information integrity policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. **Examine** the system and information integrity policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. **Examine** the system and information integrity procedures to determine if the procedures are sufficient to address all areas identified in the system and information integrity policy and all associated system and information integrity controls. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system and information integrity policy and procedures control is implemented. **Examine** the system and information integrity policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies regulations, standards, and guidance. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization consistently applies the system and information integrity policy and procedures on an ongoing basis. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the system and information integrity policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: SI-2 FLAW REMEDIATION		
The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws).	(1) The organization centrally manages the flaw remediation process and installs updates automatically without individual user intervention.	**Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization identifies recently announced software flaws and potential vulnerabilities resulting from those flaws that may affect the information system. **Examine** organizational records or documents to determine if the organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SI-2 FLAW REMEDIATION		
Proprietary software can be found in either commercial off-the-shelf information technology component products or in custom-developed applications. The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation.	(2) The organization employs automated mechanisms to periodically and upon command determine the state of information system components with regard to flaw remediation.	**Examine** organizational records or documents to determine if the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the flaw remediation control is implemented. **Examine** organizational records or documents to determine if the organization captures all appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned. **Test** the information system with automated security tools to determine the effectiveness of the organization's flaw remediation capabilities. **Examine** organizational records or documents containing a listing/log of recent security flaw remediation actions performed on the information system to determine if the system is appropriately modified to reflect the required flaw remediation. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization consistently applies flaw remediation efforts within the information system on an ongoing basis. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the flaw remediation control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization centrally manages the flaw remediation process for the information system. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization employs a centralized patch management program to assist system administrators in identifying, acquiring, testing, and deploying patches. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization installs information system software updates automatically. **Examine** the application that performs automatic updates to the information system software (or the documentation for the application) to determine how frequently automatic updates occur. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization employs automated mechanisms to determine the security posture of information systems with respect to remediation of identified flaws.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SI-3 MALICIOUS CODE PROTECTION		
The organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) transported: (i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., diskettes or compact disks), or other common means; or (ii) by exploiting information system vulnerabilities. The organization updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures.	(1) The organization centrally manages malicious code protection mechanisms. (2) The information system automatically updates malicious code protection mechanisms.	**Examine** organizational records or documents to determine if the organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses). **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** malicious code protection mechanisms to determine if the mechanisms detect and eradicate malicious code transported: (i) by electronic mail, electronic mail attachments, Internet access, removable media (e.g., diskettes, or compact discs), or other common means; or (ii) by exploiting information system vulnerabilities. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization employs malicious code protection mechanisms for applications that may transfer malicious code (e.g., file transfer software, instant messaging software). **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization updates malicious code protection mechanisms whenever new releases are available in accordance with organizational policy and procedures. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the malicious code protection control is implemented. **Examine** malicious code protection mechanisms to determine if the mechanisms are: (i) appropriately updated to include the latest malicious code definitions; (ii) configured to perform periodic scans of the information system as well as real-time scans of each file as it is downloaded, opened, or executed; and (iii) configured to disinfect and quarantine infected files. **Examine** electronic mail clients and servers to determine if the clients and servers are configured to block attachments with file extensions associated with malicious code (e.g., .pif, .vbs), and suspicious file extension combinations (e.g., .txt.vbs, .htm.exe). **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization consistently applies malicious code protection measures within the information system on an ongoing basis. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the malicious code protection control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SI-3 MALICIOUS CODE PROTECTION		
Consideration is given to using malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). NIST Special Publication 800-83 provides guidance on implementing malicious code protection.		**Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization centrally manages malicious code protection mechanisms employed in organizational information systems **Examine** the information system configuration to determine if the malicious code protection mechanisms are configured to download and install updates automatically directly from the vendor or some other trusted source.
Control Number: SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES		
Information system monitoring capability can be achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, log monitoring software, network monitoring software, network forensic analysis tools). Monitoring devices can be strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices can also be deployed at ad hoc locations within the system to track	(1) The organization networks individual intrusion detection tools into a system wide intrusion detection system using common protocols. (2) The organization employs automated tools to support near-real-time analysis of events in support of detecting system-level attacks. (3) The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to	**Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization employs information system monitoring tools and techniques to include intrusion detection systems, malicious code protection software, log monitoring software, and network forensic analysis tools. **Examine** intrusion detection tools for the information system to determine if the tools are configured and updated to detect vulnerabilities, changes to the network, both known and unknown attack signatures, and traffic anomalies. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization is appropriately staffed and operational to monitor the information system in accordance with organizational policy and procedures. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system monitoring tools and techniques control is implemented. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization consistently monitors the activity on the information system using appropriate monitoring tools and techniques on an ongoing basis. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system monitoring tools and techniques control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES		
specific transactions (See related security control AC-8 for system use notification). Additionally, these devices can be used to track the impact of security changes to the information system. The granularity of the information collected can be determined by the organization based upon its monitoring objectives and the capability of the information system to support such activities. NIST Special Publication 800-83 provides guidance on detecting malware-based attacks through malicious code protection software.	attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination. (4) The information system monitors inbound and outbound communications for unusual or unauthorized activities indicating the presence of malware (e.g., malicious code, spyware, adware).	**Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization provides the capability through the employment of automated tools, to immediately investigate, report, and respond to suspicious activity in real-time. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms. **Examine** organizational records or documents to determine if the information system monitors inbound and outbound communications for unusual or unauthorized activities indicating the presence of malware. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization reviews information system monitoring logs to assess if there is a pattern of unusual or unauthorized activities.
Control Number: SI-5 SECURITY ALERTS AND ADVISORIES		
The organization documents the types of actions to be taken in response to security alerts/advisories. The organization also maintains contact with special interest groups (e.g., information security forums) that: (i) facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies);	(1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.	**Examine** organizational records or documents (including any logs documenting alerts/advisories) to determine if the organization: (i) receives information system security alerts and advisories; (ii) disseminates the alerts and advisories to appropriate personnel; (iii) takes appropriate actions in response; and (iv) documents the results including the date and time of each action taken. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization provides the capability to immediately react and respond to new security alerts and advisories. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security alerts and advisories control is implemented. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization consistently receives and responds to security alerts and advisories for the information system on an ongoing basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SI-5 SECURITY ALERTS AND ADVISORIES		
(ii) provide access to advice from security professionals; and (iii) improve knowledge of security best practices. NIST Special Publication 800-40 provides guidance on monitoring and distributing security alerts and advisories.		**Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security alerts and advisories control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization uses automated mechanisms to automatically disseminate security alerts and advisories to appropriate personnel and how the automated mechanisms are implemented.
Control Number: SI-6 SECURITY FUNCTIONALITY VERIFICATION		
	(1) The organization employs automated mechanisms to provide notification of failed security tests. (2) The organization employs automated mechanisms to support management of distributed security testing.	**Interview** selected organizational personnel with system and information integrity responsibilities to determine if the information system verifies the correct operation of security functions upon system startup and restart, and/or upon command by users with appropriate privileges. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the information system notifies the system administrator, shuts the system down, or restarts the system when anomalies are discovered. **Examine** the system configuration to determine if it verifies the correct operations of security functions [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator, shuts the system down, restarts the system] when anomalies are discovered. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security functionality verification control is implemented. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the information system consistently verifies the security functionality within the system on an ongoing basis. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security functionality verification control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization employs automated mechanisms to provide notification of failed security tests to appropriate personnel. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization employs automated mechanisms to support management of distributed security testing.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SI-7 SOFTWARE AND INFORMATION INTEGRITY		
The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.		**Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization employs integrity verification software on the information system to look for evidence of information tampering, errors, and omissions. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization employs software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes). **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization employs tools to automatically monitor the integrity of the information system and the applications the system hosts. **Examine** information system integrity applications and tools to determine if the applications and tools effectively detect unauthorized changes to software and information. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the software and information integrity control is implemented. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the information system detects and protects against unauthorized changes to software and information on an ongoing basis. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the software and information integrity control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: SI-8 SPAM PROTECTION		
The organization employs spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network.	(1) The organization centrally manages spam protection mechanisms. (2) The information system automatically updates spam protection mechanisms.	**Examine** organizational records or documents to determine if the organization employs spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization employs spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization updates spam protection mechanisms whenever new releases are available in accordance with organizational policy and procedures. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the spam protection control is implemented.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SI-8 SPAM PROTECTION		
The organization uses the spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet accesses, or other common means. Consideration is given to using spam protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations).		**Examine** the information system's spam protection mechanism(s) by scanning critical information system entry points for the presence of spam. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization consistently applies spam protection measures within the information system on an ongoing basis. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the spam protection control are documented and the resulting information used to actively improve the control on a continuous basis. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization employs a centralized management architecture to manage spam protection mechanisms for the information system. **Examine** spam protection mechanisms to determine if the mechanisms are configured to download and install updates automatically from the vendor or some other trusted source.
Control Number: SI-9 INFORMATION INPUT RESTRICTIONS		
Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.		**Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the information system employs restrictions on personnel authorized to input information to the information system to include limitations based on specific operational/project responsibilities. **Examine** the information system to determine if user accounts are restricted from inputting information beyond the typical access controls unless specifically authorized based on operational/project responsibilities. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information input restrictions control is implemented. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization consistently restricts information system inputs to the information system on an ongoing basis. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information input restrictions control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY		
Checks for accuracy, completeness, validity, and authenticity of information should be accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to ensure that inputs match specified definitions for format and content. Inputs passed to interpreters should be prescreened to ensure the content is not unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information should be guided by organizational policy and operational requirements.		**Examine** the information system to determine if the system checks information inputs for accuracy, completeness, and validity of information as close to the point of origin as possible. **Examine** the information system to determine if the system employs rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) to ensure that inputs match specified definitions for format and content. **Examine** the information system to determine if the system prescreens inputs passed to interpreters to ensure the content is not unintentionally interpreted as commands. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information accuracy, completeness, validity, and authenticity control is implemented. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the information system consistently performs information accuracy, completeness, validity, and authenticity checks on an ongoing basis. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security functionality verification control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: SI-11 ERROR HANDLING		
The structure and content of error messages should be carefully considered by the organization.		**Examine** the information system to determine if the system identifies and handles error conditions in an expeditious manner. **Examine** the information system to determine if the system provides timely error messages that contain useful information to users without revealing information that could be exploited by adversaries. **Examine** the information system to determine if the system provides error messages only to authorized personnel (e.g., system administrators, maintenance personnel).

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: SI-11 ERROR HANDLING		
User error messages generated by the information system should provide timely and useful information to users without revealing information that could be exploited by adversaries. System error messages should be revealed only to authorized personnel (e.g., systems administrators, maintenance personnel). Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) should not be listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions should be guided by organizational policy and operational requirements.		**Examine** the information system to determine if the system lists sensitive information (e.g., account numbers, social security numbers, and credit card numbers) in error logs or associated administrative messages. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the information system provides the capability to identify and handle error conditions in compliance with organizational policy and procedures. **Examine** organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the error handling control is implemented. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the information system consistently handles error conditions on an ongoing basis. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the error handling control are documented and the resulting information used to actively improve the control on a continuous basis.
Control Number: SI-12 INFORMATION OUTPUT HANDLING AND RETENTION		
		Interview selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the information system consistently handles error conditions on an ongoing basis. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the error handling control are documented and the resulting information used to actively improve the control on a continuous basis.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Enrollment Process Class: N/a		
Control Number: EP-1 BIOGRAPHIC INFORMATION COLLECTION		
		Obtain and inspect EP kiosk physical security policies and procedures to determine whether controls are in place to prevent individuals from compromising PII. **Observe** that appropriate physical security controls are in place and operating effectively. **Verify** through observation that surveillance is present around the EP kiosks to monitor unauthorized acquisition of PII. Using a standard web browser capture the information from the website's published certificate and ensure the following standards are met: 1. Certificate is current: Review expiration date 2. Appropriate encryption is in use: **Examine** the encryption strength and type 3. Issued by an authorized certificate vendor: e.g. Thwart or Verisign **Obtain** and inspect enrollment technician standard operating procedures and evidence of training to determine whether the biographic information accuracy process is documented. **Observe** that biographic information accuracy controls are operating effectively. **Verify** audit trails uniquely identify EP personnel who verify the accuracy of biographic data and the validation of personal identification documents and that they are systematically attached to the RT Applicant's file. **Verify** field edits are accurately recorded in EP information system documentation. Process a fictitious biographic entry of an invalid date of birth, such as a DOB occurring in the future to verify field edits are operating effectively. **Obtain** and inspect EP policies and procedures to determine whether they require dual validation of personal identification documents. **Test** system controls to verify that they require dual validation of personal identification documents. **Verify** audit trails uniquely identify EP personnel who authorize the acceptance of biographic data and the validation of personal identification documents and that they are systematically attached to the RT Applicant's file.
Control Number: EP-2 DOCUMENT VALIDATION		
		Obtain and inspect EP policies and procedures regarding document validation to determine whether electronic authentication devices are required to detect fraudulent personal identification documents. **Inspect** a sample of EP locations to determine whether EP personnel utilize anti-fraud features to inspect government-issued documents. **Obtain** and inspect training policies and procedures to determine whether training regarding the identification of personal identification documents is required. **Verify** training records are maintained and select a sample to determine whether current employees received appropriate training. **Obtain** an understanding of the SP information systems. **Verify** that system controls exist which require dual validation of personal identification documents. **Verify** audit trails uniquely identify EP personnel who authorize the acceptance of biographic data and the validation of personal identification documents and that they are systematically attached to the RT Applicant's file.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: EP-3 BIOMETRIC COLLECTION		
		Obtain an understanding of the SP information systems. **Verify** that system controls exist which require dual validation of personal identification documents. **Obtain** and inspect access control and separation of duties policies to ensure authorization of biographic data and the collection of biometrics processes are separated. **Verify** systematic controls are in place and are operating effectively. **Verify** procedures are in place to monitor the chain of custody of the RT Applicant to ensure the biometric collection process is not compromised. **Verify** audit trails uniquely identify EP personnel who collect biometric data and that they are systematically attached to the RT Applicant's file. **Obtain** and inspect training policies and procedures to determine whether training regarding biometric collection is required. **Verify** training records are maintained and select a sample to determine whether current employees received appropriate training. **Obtain** an understanding of SP systems. **Verify** systematic controls are in place to ensure biometrics are captures in accordance with CIMS specifications.
Control Number: EP-4 CARD PRODUCTION AND ISSUANCE		
		Obtain an understanding of the delivery of the payload to the RT Cards. **Select** a subjective sample of cards and attempt to re-image the cards with test data using standard equipment. Expected test result: The card image will remain unchanged or the card will become permanently unusable.
Control Number: EP-5 DATA COLLECTION & STORAGE		
		Examine the archived completed electronic enrollment forms.
Control Number: EP-6 EXCESS DATA		
		Examine the RT enrollment screen/form to verify that excess data is collected in accordance with the RT Standards and is logically separated from RT required information.
Control Number: EP-7 INFORMATION PROVIDED TO AND RECEIVED FROM APPLICANT		
		Examine the enrollment form/screen to determine if the RT required information is provided to all RT applicants.
Control Number: EP-8 ENROLLMENT CONFORMANCE		
		Examine the documentation showing the entity has passed the CIMS conformance testing for enrollment services.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Verification Process Class: N/A		
Control Number: VP-1 CHECKPOINT VERIFICATION		
		Inspect a sample of VP designated areas to validate the physical location and process of verifying an RT Participant in ensuring only RT Participants are entering authorized areas and non-participants are not bypassing RT designated lanes or privileges. **Obtain** and inspect policies and procedures to determine whether controls require the RT's boarding pass is marked with a unique identifier denoting that they have been successfully verified by the VP kiosk. **Observe** the VP kiosks to ensure RT's boarding pass is marked with a unique identifier. **Obtain** and inspect VP policies and procedures to determine if the unique identifier is changed with sufficient frequency to maintain the integrity of the identifier. **Inspect** the policies and procedures to determine whether sufficient coordination is addressed to ensure the TSOs can recognize the unique identifier. **Obtain** and inspect SP policies and procedures with regards to CHRC and STA checks to determine whether they are required for all employees. **Obtain** a roster of employees and make a selection to determine CHRC and STA checks have been appropriately completed and documented.
Control Number: VP-2 VERIFICATION CONTROLS		
		Verify that systematic controls are in place which dictates a maximum number of biometric attempts before the RT Participant is rejected from verification kiosk and traveler sent to regular security lanes.
Control Number: VP-3 METRICS		
		Obtain and inspect policies and procedures, or information system documentation to verify sufficient metrics to measure false rejection rates are required. Obtain and inspect policies and procedures, or information system documentation to verify daily metrics are maintained to measure false rejection rates. Examine metrics reports to determine if they have been reported in accordance with the RT Standards.
Control Number: VP-4 VERIFICATION CONFORMANCE		
		Examine the documentation showing the entity has passed the conformance testing for verification services.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: VP-5 FALLBACK CONTROLS		
		Obtain and inspect policies or procedures to verify that they document VP kiosk operators re-route RT Participants to standard TSA screening lines in the event the VP kiosk is not functioning.
Privacy Class: N/A		
Control Number: PR-1 OPENNESS		
		Examine organizational records or documents to determine if the organization has a documented privacy policy that explicitly defines, communicates, and assigns responsibilities for privacy functions. **Interview** selected organizational personnel with privacy responsibilities to determine if key operating elements within the organization understand their privacy roles and are ready to implement the policy
Control Number: PR-2 COLLECTION LIMITATION		
		Examine the organization's privacy policy to determine if it collects information only for the purposes identified in the privacy notice, addresses the choices available to RT applicants, and requires consent with respect to the collection, use, and disclosure of personal information.
Control Number: PR-3 PURPOSE SPECIFICATION		
		Examine organizational records or documents to determine if the organization provides notice to RT applicants about its privacy policy and procedures and if it identifies how the information will be collected, used, retained, and disclosed.
Control Number: PR-4 USE LIMITATION		
		Examine the privacy policy and procedures to determine if the organization limits the use of personal information to only the purposes identified in the notice and for which the individual has provided implicit or explicit consent.
Control Number: PR-5 DATA QUALITY		
		Examine organizational records or documents to determine if the organization maintains accurate, complete, and relevant personal information.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: PR-6 INDIVIDUAL PARTICIPATION		
		Examine the privacy policy to determine if it requires that RT applicants have access to their personal information for review and update. **Examine** the organization's privacy procedures to determine if there is a complaints process in place. **Examine** the organizational records or forms that are provided to individuals to determine if they are allowed to review and update their information.
Control Number: PR-7 SECURITY SAFEGUARDS		
		Examine organizational records or documents to ensure that security measures are in place to protect privacy information.
Control Number: PR-8 ACCOUNTABILITY		
		Examine the organization's privacy procedures to determine if it monitors its compliance with the privacy policy. **Examine** organizational records or documents that indicate that compliance monitoring has taken place (i.e. self assessments, complaint reports, etc).
Registered Traveler Class: N/A		
Control Number: RT-1 SECURITY STATUS		
		Examine the procedures for RT operations to determine if the entity accepts RT Participants from all operational SPs at no additional cost to the participant. **Examine** organizational records to determine if there were instances when RT Participants were denied access to an RT Line.
Control Number: RT-2 Updates to Biographic Information		
		Examine the procedures for verifying participant identity documents whenever there is a change or update to their information.
Control Number: RT-3 RT Card Deactivation		
		Examine organizational records to determine if the entity reports when a card should be deactivated in the CIMS within 24 hours.

Supplemental Guidance	Recommended Control Enhancements	Recommended Audit Test Procedures
Control Number: RT-4 Interoperability		
		Examine the procedures for RT operations to determine if the entity accepts RT Participants from all operational SPs at no additional cost to the participant. **Examine** organizational records to determine if there were instances when RT Participants were denied access to an RT Line.
Control Number: RT-5 Approval to Operate		
		Examine organizational records to determine if an IPA firm performed an initial attestation before the SP commenced operations and annual attestations thereafter.
Control Number: RT-6 Oversight		
		Examine the entity's contract with the SE to determine if there is a provision authorizing TSA oversight and allowing TSA to audit or inspect the controls over the SP's RT Program.

Homeland Security

RT Registered Traveler™