R.I.T.A. Data Safeguards
3rd Party Print Facilities

ID	Control Name	Procedures	Expected Result	Actual Result	Status
1	Risk Assessment Policy And Procedures	1. Examine risk assessment policy and procedures. 2. Interview personnel with risk assessment responsibilities to determine how often risk assessment policy and procedures (i) are reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Examine risk assessment policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among company entities, and compliance.	1. Risk assessment policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the company. 2. Risk assessment policy and procedures (i) are periodically reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Risk assessment policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among company entities, and compliance.		
2	Risk Assessment	1. Examine the most recent risk assessment conducted on the system.	1. Ensure the system processing RITA data in within scope of the most recent risk assessment. 2. Risk assessment has been conducted and documented that includes the magnitude of harm that could result from the unauthorized access, use, disclosure, modification, or destruction of the RITA's information and the information systems that support its operations and assets (including information and information systems managed/operated by external parties).		
3	Risk Assessment Update	1. Examine risk assessment policy and procedures to determine how often risk assessments are updated. 2. Examine the most recent risk assessment conducted on the system and interview personnel with risk assessment responsibility to determine if the report reflects the latest significant changes.	1. The risk assessment is updated at a minimum of three years or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security status of the system. 2. The risk assessment was performed within the last three years and reflects the latest significant changes to the information system, the facilities where the system resides, or other conditions that may have impacted the security status of the system..		
4	Vulnerability Scanning	Procedures: 1. Examine risk assessment policy and procedure and interview personnel with risk assessment responsibility to determine how often the system is scanned for vulnerabilities. 2. Examine the latest vulnerability scanning results report. 3. Examine the scanning tool used by the company to verify its functionality.	1. The company scans the information system for vulnerabilities quarterly or when significant new vulnerabilities are identified and reported. 2. The vulnerability scan was conducted within the last quarter, or more recently. 3. The company uses scanning tools that ensure interoperability among tools and automate parts of the vulnerability management process by using standards for (a) enumerating platforms, software flaws, and improper configurations, (b) formatting and making transparent checklists and test procedures, and (c) measuring vulnerability impact.		
5	Security Planning Policy And Procedures	1. Examine security planning policy and procedures. 2. Interview company personnel with security planning responsibilities to determine how often security planning policy and procedures (i) are reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Examine security planning policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among company entities, and compliance.	1. Security planning policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the company. 2. Security planning policy and procedures (i) are periodically reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Security planning policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among company entities, and compliance.		
6	System Security Plan	1. Examine the most recent system security plan for the system(s) processing RITA's information.	1. The security plan provides an overview of the security requirements for the information system and a description of the security controls planned or in place for meeting the security requirements. 2. Designated company officials have reviewed and approved the security plan.		
7	System Security Plan Update	1. Examine security planning policy and procedures to determine how often the security plan is reviewed and updated. 2. The System Security Plan should be reviewed annually.	1. The system security plan is reviewed annually. During reviews, major changes to the company, information system and problems with security plan implementation and security control enhancements are considered for updates. 2. Interviewee should be able to show documentation that this review has taken place.		
8	Acceptable Use	1. Examine the acceptable use policy around the information systems that process RITA's data. 2. Interview an authorized system user to determine their awareness of the acceptable use policy. 3. Examine user's signed acceptable use policy.	1. The Rules of Behavior establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage. 2. The user is aware of the Rules of Behavior, and the document is readily available to them. 3. The Rules of Behavior document is signed, indicating acknowledgement from the user that they have read, understand, and agree to abide by the rules of behavior.		
9	Security-Related Activity Planning	1. Examine security planning policy and procedures and interview personnel with security planning responsibility to determine if system security related activities are properly coordinated.	1. Security-related activities including, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises are coordinated prior to execution to limit the impact on company operations.		
10	System And Services Acquisition Policy And Procedures	1. Examine system services and acquisition policy and procedures. 2. Interview company personnel with system services and acquisition responsibilities to determine how often system services and acquisition policy and procedures (i) are reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Examine system services and acquisition policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among company entities, and compliance.	1. System services and acquisition policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the company. 2. System services and acquisition policy and procedures (i) are periodically reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. System services and acquisition policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among company entities, and compliance.		
11	Allocation of Resources	1. Examine system services and acquisition policy and interview company personnel with services and acquisition responsibility to determine how resources are allocated for system security requirements/mechanisms. 2. Examine information system business case planning and budgeting documentation.	1. The organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system; 2. The organization determines security requirements for the information system in mission/business case planning. A discrete line item for information system security is established in the organization's programming and budgeting documentation.		

ID	Control Name	Procedures	Expected Result	Actual Result	Status
12	Life Cycle Support	1. Examine information system development life cycle documentation. 2. Examine the company's system development life cycle. (Only applicable if software if custom software is developed and used to process RITA's data)	1. The company manages the system using a system development life cycle methodology that includes information security considerations. 2. The company uses a system development life cycle that is consistent with the following phases: initiation, acquisition/development, implementation, operations/maintenance, and disposition. Each of these five phases includes a minimum set of security steps to effectively incorporate security into a system during its development. Note: The company will either use the general SDLC described in the expected result or will have developed a tailored SDLC that meets their specific needs. In either case, security steps shall be incorporated into the company's SDLC.		
13	Acquisitions	1. Examine system acquisition documentation, including acquisition contracts for the information system or services. 2. Examine system acquisition documentation to determine if guidance is provided on the acquisition and use of tested/evaluated information technology products.	1. Acquisition contracts for information systems include, either explicitly or by reference, security requirements and/or security specifications that describe: -required security capabilities; -required design and development processes; -required test and evaluation procedures; and -required documentation. 2. The company gives substantial consideration to procuring commercial IT products that have been evaluated and tested by independent accredited laboratories against appropriate security specifications and requirements.		
14	Information System Documentation	1. Examine information system documentation, including administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system’s security features. 2. Interview personnel operating, using or maintaining the system to verify information system documentation is made available. 3. Examine the location of information system documentation, either in hard copy or soft copy.	1. Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system’s security features. 2. Operational personnel has knowledge of, and an available copy of the documentation. 3. Information system documentation is made available to authorized personnel only.		
15	Software Usage Restrictions	1 & 2. Examine the list of software usage restrictions. 3. Examine inventory of licensed software installed on the system, and site software license documentation.	1. The policy mandates a regular review of software usage for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. 2. The policy controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used in the processing of RITA's information. 3. Only licensed and approved software is contained in the inventory of software installed on the system. The company makes use of a controlled implementation process for licensed software and employs tracking systems to control copying and distribution.		
16	User Installed Software	1. Examine software usage restriction policy and/or list of rules governing user installed software.	1. The company enforces explicit rules via a written policy governing the installation of software by users. The policy identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software that is free only for personal, not government use, and is potentially malicious). The company regularly reviews/analyzes user installed software for indications of inappropriate or unusual activity.		
17	External Information System Services	1. Interview company personnel to determine if information system services for systems that store, process or transmit RITA data are implemented by a provider external to the company. 2. Interview company personnel to determine if the company monitors security control compliance of external information system providers. 3. Use of the third party provider was disclosed to RITA as part of the contract for services.	1. If information system services are implemented by an external provider, the company requires that providers of external information system services employ adequate security controls, including how data is handled and protected at the external site, including any information stored, processed, or transmitted using the provider's computer systems; the background investigation and/or clearances requirements for external providers with access to data, and security awareness and training requirements for external providers with access to data. 2. The company regularly reviews/analyzes external providers of 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. 3. Disclosure of the use of the third party any portion of the processing lifecycle of RITA's data was properly disclosed and approved in the services contract.		
18	Developer Security Testing	1. Interview company personnel to determine if security test and evaluations are performed during system development. 2. Examine security test and evaluation plan and results from system development, or the most recent modification to the system. *** This is only applicable if custom developed software is maintained and used by the vendor in the processing of RITA's information ***	1. The company requires that information system developers (and systems integrators) create a security test and evaluation plan, implement the plan, and document the results for newly developed systems and modifications to existing systems that impact security controls. 2. Security test and evaluation plan and results are available and document the test cases executed and results of each test.		
19	Security Assessment Policy And Procedures	1. Examine Certification, Accreditation, And Security Assessment policy and procedures. 2. Interview company personnel with Certification, Accreditation, And Security Assessment responsibilities to determine how often Certification, Accreditation, And Security Assessment policy and procedures (i) are reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Examine Certification, Accreditation, And Security Assessment policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among company entities, and compliance.	1. Certification, Accreditation, And Security Assessment policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the company. 2. Certification, Accreditation, And Security Assessment policy and procedures (i) are periodically reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Certification, Accreditation, And Security Assessment policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among company entities, and compliance.		
20	Security Assessments	1. Examine the results from the last security control assessment and determine whether the company conducts security assessments annually, or when a major change occurs. 2. Examine the results from the last security control assessment to determine if the security controls are assessed for correct implementation, for intended operation, and for producing the desired outcome with respect to meeting the security requirements for the system.	1. The results from the last security control assessment are available and an assessment of the security controls in the information system is conducted annually, or when a major change occurs. 2. Security controls are assessed for correct implementation and meet the security requirements for the system.		

R.I.T.A. Data Safeguards
3rd Party Print Facilities

ID	Control Name	Procedures	Expected Result	Actual Result	Status
21	Information System Connections	1. Examine a list of all connections connected to the information system outside of its boundary. 2. Examine remote access agreements to determine if the agreements are in place and spell out the acceptable use of the remote connection.	1. The information system has all required remote access agreements for all connections external to the system boundary. 2. The company authorizes all connections from the information system to external information systems through the use of system connection agreements that include: Interconnection statement of requirements which addresses the requirement for the interconnection, the names of the systems being connected and the company that initiated the interconnection.		
22	Security Certification	1. Examine the most recent security assessment plan, results and report. 2. Examine procedures addressing security certification to determine if the company employs a security certification process whereby the system owner reviews the results of the security assessments and approves or denies the deployment of the system to production.	1. The company conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. 2. The company employs security certification process. The company assesses all security controls in an information system during the initial security accreditation. The system owner reviews the results of the most recent assessment and approves or denies the implementation of the system into production.		
23	Plan Of Action And Milestones	1. Examine the system remediation plan corresponding to the last security control assessment.	1. The system remiadiation plan documents the planned, implemented, and evaluated actions to correct the deficiencies and vulnerabilities in the system identified from audits, assessments, and known vulnerabilities, and was updated with results from the most recent security control assessment.		
24	Security Accreditation	1. Examine the security accreditation documentation. 2. Examine company security accreditation policy to verify policy for conducting accreditation when there is a major system change.	1. The accreditation documentation contains the accreditation memo, or equivalent document signed by the system owner authorizing the system for processing. 2. The company updates the authorization when there is a significant change to the information system.		
25	Continuous Monitoring	1. Examine policy and procedures addressing continuous monitoring of system security controls. 2. Examine policy and procedures addressing continuous monitoring of system security controls, examine security impact analyses. 3. Examine policy and procedures addressing continuous monitoring of system security controls	1. Continuous monitoring policy and procedures address configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. the organization assesses a subset of the controls annually during continuous monitoring. 2. The company conducts security impact analyses on changes to the information system; the company documents and reports changes to the security controls employed in the system and updates the system security plan and system remediation plan as appropriate based on outcome of continuous monitoring activities. 3. The policy establishes the selection criteria and subsequently selects a subset of the security controls employed within the information system for assessment.		
26	Personnel Security Policy And Procedures	1. Examine personnel security policy and procedures. 2. Interview company personnel with personnel security responsibilities to determine how often personnel security policy and procedures (i) are reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Examine personnel security policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among company entities, and compliance.	1. Personnel security policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the company. 2. Personnel security policy and procedures (i) are periodically reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Personnel security policy should address the following areas: Position Categorization, Personnel Screening, Personnel Termination, Personnel Transfer, and Access Agreements. Personnel security policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among company entities, and compliance.		
27	Position Categorization	1. Examine a list of risk designations for company positions that require access to data. 2. Examine the personnel security policy to verify the screening criteria. 3. Examine the personnel security policy to verify the frequency that position descriptions are reviewed and updated.	1. The company assigns a risk designation to all positions requiring access to RITA data. 2. The company establishes a screening criteria for individuals filling organizational positions requiring access to RITA data. 3. The company reviews and revises position risk designations in accordance with the company personnel security policy.		
28	Personnel Screening	1. Examine applicable documents to determine if the company appropriately screens individuals requiring access to RITA information and information systems prior to authorizing access. 2. Examine a sample of the personnel records to verify that each employee was subject to background screening in accordance with company personnel policy before being granted information system access.	1. The company screens individuals requiring access to company information systems containing data prior to authorizing access. 2. Each of the new employees was subject to the appropriate background screening before they were granted information system access.		
29	Personnel Termination	1. Examine company employee termination procedures and interview company employees with personnel security responsibility. 2. Examine a list of recently terminated employees and verify that records of personnel termination exist for those employees.	1. The company terminates information system access upon termination of individual employment, conducts exit interviews of terminated personnel, retrieves all organizational information system-related property, e.g., keys, identification cards, and building passes from terminated personnel, and retains access to official documents and records on organizational information systems created by terminated personnel. 2. All terminated employees on the list have an associated record of termination activities performed in accordance with company policy.		
30	Personnel Transfer	1. Examine company employee transfer procedures and interview company employees with personnel security responsibility.. 2. Examine a list of recently transferred employees and verify that records of personnel transfer exist for those employees.	1. The company (i) reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the company; and (ii) initiates the following appropriate actions: 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. 2. All transferred employees on the list have an associated record of transfer activities performed in accordance with company policy.		
31	Access Agreements	1. Examine a list of employee access agreements (e.g., nondisclosure agreements, acceptable use agreements, conflict-of-interest agreements) for current employees who have access to systems containing RITA data.	1. Employees access agreements are signed before being authorized access to systems containing RITA data.		

ID	Control Name	Procedures	Expected Result	Actual Result	Status
32	Third Party Personnel Security	1. Interview company personnel to determine if third-party providers (e.g., third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management.) are utilized by the company for systems containing RITA data. 2. Examine acquisition related documents (e.g., contracts, service level agreements) for the third party provider to verify personnel security requirements are included. 3. Interview company personnel with personnel security responsibility and examine compliance reports to verify techniques for monitoring compliance with personnel security requirements.	1. If no third party providers are utilized, this control can be marked N/A. If third party providers are utilized, proceed to test procedure number 2. 2. Acquisition related documents contain requirements for the third party provider to ensure they must follow company personnel security requirements. 3. The company uses mechanisms such as compliance reports to ensure the third party provider complies with company personnel security requirements.		
33	Personnel Sanctions	Procedures: 1. Examine personnel security policy and information system acceptable use documents.	1. The policy and rules of behavior documents contain a formal sanctions process for personnel failing to comply with company information security policies and procedures.		
34	Contingency Planning Policy And Procedures	1. Examine contingency planning policy and procedures. 2. Interview company personnel with contingency planning responsibilities to determine how often contingency planning policy and procedures (i) are reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Examine contingency planning policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among company entities, and compliance.	1. Contingency planning policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the company. 2. Contingency planning policy and procedures (i) are periodically reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Contingency planning policy should address the following areas: Alternate Storage Sites, Telecommunication Services, and Information System Backup.		
35	Contingency Plan	1. Examine the IT Contingency Plan (ITCP) for the information system(s) processing, storing or transmitting RITA data. 2. Examine procedures addressing contingency operations for the information system(s).	1. The ITCP addresses contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system. 2. The contingency plan is reviewed and approved by designated organizational officials, and disseminated to key personnel with contingency planning responsibility.		
36	Contingency Plan Testing and Exercises	1. Examine contingency plan testing and/or exercise documentation. 2. Examine contingency plan testing records documents the results of contingency plan testing/exercises.	1. The company defines the set of contingency plan tests and/or exercises, and tests/exercises the contingency plan annually. 2. Testing records document the results of contingency plan testing/exercises.		
37	Contingency Plan Update	1. Examine contingency planning policy to determine ITCP update schedule.	1. The company updates the contingency plan at least annually based on experiences during plan implementation, execution, and testing.		
38	Alternate Storage Site	1. Examine procedures addressing alternate storage sites, or interview personnel with alternate storage site responsibility. 2. Examine alternate storage site agreements.	1. The company identifies an alternate storage site; 2. The alternate storage site agreements are currently in place, available, accessible, and meets the requirements (including necessary equipment and supplies) to permit the storage of information system backup.		
39	Alternate Processing Site	1. Examine procedures addressing alternate processing sites, or interview personnel with alternate processing site responsibility. 2. Examine alternate processing site agreements.	1. The company identifies an alternate processing site. 2. Alternate processing site agreements are currently in place to permit the resumption of information system operations for critical mission/business functions, and defines the time period within which processing must be resumed at the alternate processing site.		
40	Configuration Management Policy And Procedures	1. Examine configuration management policy and procedures. 2. Interview company personnel with configuration management responsibilities to determine how often configuration management policy and procedures (i) are reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Examine configuration management policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among company entities, and compliance.	1. Configuration management policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the company. 2. Configuration management policy and procedures (i) are periodically reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required.		
41	Baseline Configuration	1/2. Examine the information system baseline configuration.	1. The company maintains a documented baseline configuration of the information system that provides the organization with a well-defined and documented specification to which the information system is built (e.g., software versions, patch level) 2. The baseline configuration includes documented deviations from the baseline configuration.		
42	Configuration Change Control	1. Examine configuration management policy and procedures and company configuration management plan. 2. Examine change request documentation for specific information systems changes.	1. The company manages configuration changes to the information system using an organizationally approved process (e.g., a chartered Configuration Control Board) that includes an approval process for emergency changes. 2. The change request documentation shows that the company authorizes, documents, and controls changes to the information system.		
43	Monitoring Configuration Changes	1. Examine change request documentation for specific system changes.	1. The change request documentation includes an analysis for potential security impacts, and after the change is implemented, (including upgrades and modifications), the functionality of the security features are verified to still be functioning properly.		
44	Access Restrictions For Change	1/2. Examine the list of personnel authorized access to the information system for the purpose of initiating changes.	1. The company maintains a list of qualified and authorized personnel permitted to access the information system for the express purpose of initiating changes. the ability to make configuration changes is restricted to authorized development and configuration management staff only and list of the staff is maintained. 2. The company generates, retains, and reviews records reflecting all such changes to the information system.		

ID	Control Name	Procedures	Expected Result	Actual Result	Status
45	Configuration Settings	1. Examine configuration management policy. 2. Examine platform specific secure configuration guidance to determine if system configurations follow configuration management policy.	1. The company establishes and documents mandatory configuration settings for information technology products employed within the information system. 2. The company configures the security settings of information technology products to the most restrictive mode consistent with operational requirements.		
46	Least Functionality	1. Examine configuration management policy and platform specific secure configuration guidance.	1. The company identifies prohibited or restricted functions, ports, protocols, and services for the information system.		
47	Information System Component Inventory	1. Examine current inventory of information system components.	1. The company develops, documents, and maintains a current inventory of the components of the information system and includes appropriate information to track components (e.g., manufacturer, model number, serial number, software license information, system/component owner).		
48	System Maintenance Policy And Procedures	1. Examine system maintenance policy and procedures. 2. Interview company personnel with system maintenance responsibilities to determine how often system maintenance policy and procedures (i) are reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Examine system maintenance policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among company entities, and compliance.	1. System maintenance policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the company. 2. System maintenance policy and procedures (i) are periodically reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. System maintenance policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among company entities, and compliance.		
49	Controlled Maintenance	1. Examine system maintenance schedule/records to determine if preventive and regular maintenance on the components of system is done in accordance with manufacturer or vendor specification and/or company requirements. 2. Examine system maintenance procedures and interview personnel with system maintenance responsibility to determine procedures for removal of information system components from the facility for repair. 3. Verify the equipment with media used to store or process RITA information if properly destroyed or sanitized before the component is sent offsite for repair or replaced.	1. Routine preventative maintenance is performed regularly and in accordance with guidance from the vendor. 2. Company officials approve the removal of the information system or information system components from the facility when repairs are necessary. All information is removed from associated media using company approved procedures. 3. Media installed in the system component is properly sanitized in accordance with NIST SP800-88 before component is removed from the facilitiy or is replaced due to upgrade for failure.		
50	Maintenance Tools	1. Examine maintenance tools and associated approval documentation. 2. Examine system maintenance policy.	1. All maintenance tools are approved, and include hardware and software brought into the information system specifically for diagnostic/repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). 2. The company approves, controls, and monitors the use of information system maintenance tools.		
51	Remote Maintenance	1. Interview personnel with maintenance responsibility to determine if remote maintenance activities are performed on the system. 2. Examine remote maintenance records. 3. Examine remote maintenance session configuration settings. 4. Examine system maintenance policy and procedures. 5. Vendors with remote access to information systems that process RITA data were identified and listed in the services agreement signed with RITA.	1. Remote maintenance and diagnostic activities are conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). 2. The company maintains records for all remote maintenance and diagnostic activities. 3. Remote maintenance sessions are protected with: (i) encryption and decryption of communications; (ii) strong identification and authentication techniques; and (iii) remote disconnect verification. 4. If password-based authentication is used to accomplish remote maintenance, the organization changes the passwords following each remote maintenance service.		
52	Maintenance Personnel	1. Examine procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel.	1. Only authorized personnel are authorized to perform maintenance on the information system. Maintenance personnel have appropriate access authorizations to the information system. 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.		
53	System And Information Integrity Policy And Procedures	1. Examine system and information integrity policy and procedures. 2. Interview company personnel with system and information integrity responsibilities to determine how often system and information integrity policy and procedures (i) are reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Examine system and information integrity policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among company entities, and compliance.	1. System and information integrity policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the company. 2. System and information integrity policy and procedures (i) are periodically reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. System and information integrity policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among company entities, and compliance.		
54	Malicious Code Protection	1. Examine malicious code protection mechanisms (e.g., spam/spyware and virus protection) and network design diagrams to verify the location of malicious code protection mechanisms. 2. Examine malicious code protection mechanisms configuration settings. 3. Examine malicious code protection mechanisms and records of malicious code protection updates to verify the capability to automatically update malicious code definitions is in use.	1. The company 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. 2. The company 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., USB devices, diskettes or compact disks), and are configured to perform periodic scans of the information system as well as real-time scans of files from external sources. 3. The company updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available. The most current available definition file is in use.		
55	Information System Monitoring Tools and Techniques	Procedures: 1. Examine information system design documentation to determine if the company employs information system monitoring tools and techniques to 2. Examine information system design documentation to determine the location of information system monitoring tools within the network.	1. The system has intrusion detection capability which may include the following: intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software. 2. Monitoring devices are strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices are also deployed at ad hoc locations within the system to track specific transactions.		

ID	Control Name	Procedures	Expected Result	Actual Result	Status
56	Security Alerts and Advisories	1. Examine procedures addressing security alerts and advisories and records of security alerts and advisories to determine how the company receives information system security alerts and advisories. 2. Examine procedures addressing security alerts and advisories and records of security alerts and advisories to determine actions taken in response to security alerts and advisories..	1. Company personnel with security alert/advisory responsibility subscribe to third-party vulnerability mailing lists and vendor mailing lists that highlight the most critical vulnerabilities (e.g., the US-CERT Cyber Security Alerts). 2. Security alerts and advisories are issued to appropriate company personnel, who determine the significance of the threat or vulnerability; establish which systems are vulnerable or exposed; evaluate the impact on the systems, the company and network if the vulnerability is not removed and is exploited; determine the risks involved with applying the patch or non-patch remediation; identify whether the fix will affect the functionality of other software applications or services through research and testing and make a determination on whether or not to apply a fix or not.		
57	Information Output Handling And Retention	1. Examine procedures addressing information system output handling and retention to determine how the company handles RITA data output from the information system (output includes paper and digital media).	1. Output from the system that includes RITA is handled in accordance with labeled or marked instructions on information system output (including paper and digital media) that includes, but not limited to, special instructions for dissemination, distribution, transport, or storage of information system output.		
58	Incident Response Policy And Procedures	1. Examine incident response policy and procedures. 2. Interview company personnel with incident response responsibilities to determine how often incident response policy and procedures (i) are reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Examine incident response policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among company entities, and compliance. Note: The focus of the IR controls evaluation should be surrounding the RITA data and not related to the entities' entire operation.	1. Incident response policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the company. 2. Incident response policy and procedures (i) are periodically reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Incident response policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among company entities, and compliance.		
59	Incident Response Training	1. Examine procedures addressing incident response training to determine if the company identifies and documents personnel with significant incident response roles and responsibilities. 2. Examine incident response training records to determine the frequency of training. 3. Examine the incident response training material to determine if the material addresses the procedures and activities necessary to fulfill incident response roles and responsibilities.	1. The company identifies and documents personnel with significant incident response roles and responsibilities. 2. The company provides incident response training to personnel with incident response roles and responsibilities. Initial training is provided, and refresher training is provided at least annually. 3. The incident response training material addresses the procedures and activities necessary to fulfill the incident response roles and responsibilities.		
60	Incident Response Testing and Exercises	1. Examine incident response testing policy and procedures addressing incident response testing and exercises and incident response testing material to determine the tests/exercises defined by the company. 2. Examine procedures addressing incident response testing and exercises to determine the frequency and types of test/exercises for incident response testing. 3. Examine incident response test results to verify results are documented.	1. The company defines incident response tests/exercises that contain procedures for the following: - Detecting unauthorized RITA data access - Reporting unauthorized custer data access to the RITA and internal company incident response team. 2. The company tests/exercises the incident response capability for RITA data related security violations (e.g. simulated successful unauthorized access to RITA data) at least annually. Note: The incident response tests/exercise should be different from any testing activities perform as part of Disaster Recovery or Contingency Planning. 3. The company documents the results of incident response tests/exercises.		
61	Incident Handling	1. Examine procedures addressing incident handling capability.	1. Company incident response procedures address an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery and post-incident activity.		
62	Incident Monitoring	1. Examine incident response records and documentation to determine the company's incident tracking capability.	1. The company tracks and documents information system security incidents on an ongoing basis.		
63	Incident Reporting	1. Examine incident reporting records and documentation to determine if the company promptly reports incident information to appropriate authorities. 2. Examine incident reporting records and documentation to determine if the personnel reports weaknesses and vulnerabilities in the information system to company officials in a timely manner.	1. The company promptly reports incident information involving a compromise of RITA data to the RITA. 2. In addition to incident information, weaknesses and vulnerabilities in the information system are reported to appropriate companyy officials in a timely manner to prevent security incidents.		
64	Incident Response Assistance	1. Examine company incident response procedures and/or interview company personnel with incident response responsibility to determine if the company provides an incident response support resource for assistance in handling and reporting security incidents.	1. The company provides an incident response support resource for users. Possible implementations of incident response support resources include a help desk or an assistance group, and access to forensics services.		
65	Security Awareness And Training Policy And Procedures	1. Examine security awareness and training policy and procedures. 2. Interview company personnel with security awareness and training responsibilities to determine how often security awareness and training policy and procedures (i) are reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Examine security awareness and training policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among company entities, and compliance.	1. Security awareness and training policy and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the company. 2. Security awareness and training policy and procedures (i) are periodically reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Security awareness and training policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among company entities, and compliance.		

ID	Control Name	Procedures	Expected Result	Actual Result	Status
66	Security Awareness	Procedures: 1. Examine security awareness and training policies, procedures and records 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 at least annually. 2. Examine security awareness and training materials to determine if the materials address the requirements of the company.	1. 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 at least annually. 2. The annual IT security awareness training for company employees addresses the security awareness and training requirements for employees of the company. Security awareness training identifies employees with significant information security responsibilities for systems storing, processing or transmitting RITA data, and providing role-specific training, providing annual security awareness to users of systems containing RITA data, and providing refresher training on an annual basis.		
67	Security Training	Procedures: 1. Examine security training policies, procedures and records to determine if the company identifies personnel with significant information system security responsibilities and documents those roles and responsibilities. 2. Examine security training policies, procedures and records to determine if: (i) the company 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) provides refresher training when required by system changes and annually thereafter. 3. 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. 4. Obtain a copy of the document that lists personnel who have been identified as having key information system security roles and responsibilities.	1. The company identifies personnel with significant information system security responsibilities and documents those roles and responsibilities. 2. The company provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system; records include the type of security training received and the date completed; and provides refresher training when required by system changes and annually thereafter. 3. The security training material addresses the procedures and activities necessary to fulfill those roles and responsibilities. 4. The document provides a listing of employees who have been identified as having key information system security roles and responsibilities.		
68	Security Training Records	Procedures: 1. Examine security awareness and training policy, procedures addressing security training records, security awareness and training records, and other relevant documents to determine if the company monitors and fully documents basic security awareness training and specific information system security training. 2. Inspect the training records of employees and verify that each has up-to-date security training records on file. 3. Examine applicable documents, to determine if the company documents the requirement to maintain security training records for contractors.	1. The company monitors and fully documents basic security awareness training and specific information system security training. 2. Each user has a training record that (i) identifies security training courses is taken and (ii) the record is being maintained and updated. 3. Contractors are required to complete the mandatory security training.		
69	Identification And Authentication Policy And Procedures	Procedures: 1. Examine identification and authentication policy and procedures. 2. Interview company personnel with identification and authentication responsibilities to determine how often identification and authentication policy and procedures (i) are reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Examine identification and authentication policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among company entities, and compliance.	1. Identification and authentication policies and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the company. 2. Identification and authentication policy and procedures (i) are periodically reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Identification and authentication policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among company entities, and compliance.		
70	Identifier Management	1. Examine a list of information system accounts for each system platform in scope for the computer security review. 2. Examine procedures addressing information system account access authorization. 3. Examine policy and procedures addressing dormant information system accounts. 4. Examine user account archive for each system platform in scope for the computer security review.	1. All user identifiers are unique. **Yes** 2. As part of the account authorization procedures, authorization to issue a user account to an individual from an appropriate office (e.g., manager) is received and the identify of each user is verified prior to account access being authorized. The user identifier (i.e., user ID) is issued directly to the user. **Manager** 3. User IDs are disabled after 90 days of inactivity on the information system. **Max 30 days.** 4. User IDs are deleted.		
71	Authenticator Management	1. Examine policy and procedures addressing password composition. 2. Examine procedures addressing user account management and password distribution.	1. Policy states passwords are required to be a minimum length of 8 characters in a combination of alpha and numeric or special characters. 2. Procedures for initial password distribution to new users, for replacing forgotten/compromised password passwords and revoking passwords are included.		
72	Access Control Policy And Procedures	1. Examine access control policy and procedures. 2. Interview company personnel with access control responsibilities to determine how often access control policy and procedures (i) are reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Examine access control policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among company entities, and compliance.	1. Access control policies and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the company. 2. Access control policy and procedures (i) are periodically reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Access control policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among company entities, and compliance.		

ID	Control Name	Procedures	Expected Result	Actual Result	Status
73	Remote Access	1. Check for direct internet connections e.g. (DSL) to RITA data hosting or processing platforms. 2. If a direct remote connection exists, verify the mechanisms used to monitor and control this connection.	1. There are NO direct internet connections to the platform hosting or processing RITA data. All connections originating from a remote network go through an company managed access point, e.g., VPN. 2. If a direct remote connection exists verify there is documented authorization with management sign-off, the connection is encrypted and the connection is monitored as part of the company's audit monitoring strategy.		
74	Wireless Access Restrictions	1. Examine procedures addressing wireless implementation and usage (including restrictions), activities related to wireless authorization, monitoring, and control, information system audit records and other relevant documents or records to determine if the company: i. establishes usage restrictions and implementation guidance for wireless technologies ii. documents, monitors, and controls wireless access to the information system iii. authorizes the use of wireless technologies. 2. Examine policy and procedures addressing wireless implementation and usage (including restrictions) and other relevant documents or records to determine if the access control policy and procedures address usage, implementation, monitoring, and authorization of wireless technologies. 3. Examine procedures addressing wireless implementation and usage (including restrictions), activities related to wireless authorization, monitoring, and control, information system audit records and other relevant documents or records to determine if wireless users have been authorized to access the information system. 4. Examine procedures addressing wireless implementation and usage (including restrictions), activities related to wireless authorization, monitoring, and control, information system audit records and other relevant documents or records to determine if wireless access is only permitted through the use of authentication with encryption.	1. A documented usage restriction and implementation guidance exist and wireless are access and controls are monitored. Additionally the company requires authorization before the user of wireless technologies. 2. The company wireless access control policies are consistent with NIST Wireless Network Security Policies by addressing encryption of communications, device authentication, physical security, replay protection, and wireless intrusion detection and prevention systems. 3. Wireless users have been authorized to access the information system. 4. Wireless access is only permitted through the use of authentication with encryption.		
75	Access Control for Portable and Mobile Devices	1. Examine access control policy, procedures addressing access control for portable and mobile devices, information system design documentation, information system audit records and other relevant documents or records to determine if the company: i. defines a mandatory suite of protective software and security protocols to be installed on and executed by the information system and portable and mobile devices ii. establishes and documents restrictions and implementation guidance for portable and mobile devices iii. monitors and controls the use of portable and mobile devices iv. appropriate company officials authorize the use of portable and mobile devices and device access to company information systems. v. *** The company is prohibited from storing RITA data on Portable and Mobile devices. 2. Interview company personnel with access to the information system and examine company 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 company policy and procedures. 3. Examine access control policy, procedures addressing access control for portable and mobile devices, information system design documentation and other relevant documents or records to determine if removable hard drives or encryption is used to protect information on portable and mobile devices.	1. The company: i. defines a mandatory suite of protective software and security protocols to be installed on and executed by the information system and portable and mobile devices, ii. establishes and documents restrictions and implementation guidance for portable and mobile devices and iii. monitors and controls the use of portable and mobile devices. iv. appropriate company officials authorize the use of portable and mobile devices and device access to company information systems. 2. Company personnel comply with portable and mobile device policies and procedures and compliance is monitored and enforced. 3. Information on portable devices is protected using cryptography.		

ID	Control Name	Procedures	Expected Result	Actual Result	Status
76	Use of External Information Systems	1. Examine access control policy, procedures addressing the use of external information systems, external information systems terms and conditions, list of types of applications accessible from external information systems, maximum FIPS 199 impact level for information processed, stored, or transmitted on external information systems, information system configuration settings and associated 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 RITA 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).	1. The use of personally-owned information systems to access RITA information systems is not allowed.		
77	Audit And Accountability Policy And Procedures	1. Examine audit and accountability policy and procedures. 2. Interview company personnel with audit and accountability responsibilities to determine how often audit and accountability policy and procedures (i) are reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Examine audit and accountability policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among company entities, and compliance.	1. Audit and accountability policies and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the company. 2. Audit and accountability policy and procedures (i) are periodically reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Audit and accountability policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among company entities, and compliance.		
78	Audit Reduction and Report Generation	1. Interview personnel with system audit monitoring responsibility to determine if a capability for audit reduction and report generation is implemented. 2. Examine the audit reduction and report generation tool used, as well as a sample audit report.	1. Audit reduction and report generation capability is provided either by the system itself, or by a third party software tool. 2. Examination of the tool and report indicates the tool is functioning properly.		
79	Audit Retention	1. Examine procedures addressing audit record retention. 2. Examine system audit records to verify the retention period.	1. The procedures define the retention period for audit records generated by the information system. 2. The company retains information system audit records for the company-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.		
80	System And Communications Protection Policy And Procedures	Procedures: 1. Examine system and communications protection policy and procedures. 2. Interview company personnel with system and communications protection responsibilities to determine how often system and communications protection policy and procedures (i) are reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. Examine system and communications protection policy and procedures to determine if they addresses purpose, scope, roles, responsibilities, management commitment, coordination among company entities, and compliance.	Expected Results: 1. System and communications protection policies and procedures (i) exist; (ii) are documented; (iii) and are disseminated to appropriate elements within the company. 2. System and communications protection policy and procedures (i) are periodically reviewed by responsible parties within the company; and (ii) are updated, when company review indicates updates are required. 3. System and communications protection policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among company entities, and compliance.		

ID	Control Name	Procedures	Expected Result	Actual Result	Status
81	Boundary Protection	Procedures: 1. Examine system and communications protection policy, procedures addressing boundary protection, information system design documentation, boundary protection hardware and software, information system architecture and configuration documentation, information system configuration settings and associated documentation, and other relevant documents or records to determine if the: (i) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. (ii) the company physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces. (iii) the company prevents public access into the organization's internal networks except as appropriately mediated. (iv) the company limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic. (v) the company defines the security controls (i.e., boundary protection devices and architectural configuration of the devices) appropriate at each external interface to a telecommunication service and mplements a managed interface with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted. (vi) the information system denies network traffic by default and allows network traffic by exception.	Expected Results: 1. The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. 2. The company physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces and prevents public access into the organization's internal networks except as appropriately mediated. 3. The company prevents public access into the organization's internal networks except as appropriately mediated. 4. The company limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic. 5. The company defines the security controls (i.e., boundary protection devices and architectural configuration of the devices) appropriate at each external interface to a telecommunication service and mplements a managed interface with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted. 6. The information system denies network traffic by default and allows network traffic by exception.		
82	Transmission Integrity	Procedures: 1. Examine network design diagram and interview company personnel to determine if RITA data is encrypted when transmitted across a Wide Area Network (WAN). 2. Examine network design diagram and interview company personnel to determine if RITA data is encrypted when transmitted across the Local Area Network (LAN). 3. If encryption is not used, interview company personnel to determine how RITA data is protected while in transit over the LAN and WAN.	1. Transmissions are encrypted using a key no less than 128 bits in length, or FIPS 140-2 compliant, whichever is stronger. 2. If encryption is not used to transmit data over the LAN, the company must use other compensating mechanisms (e.g., switched vLAN technology, fiber optic medium, etc.)		
83	Transmitting RITA Data - All RITA data must be protected when transmitted across a WAN or within a LAN.	Procedures: 1. If dedicated circuits are used in place of encryption for transmission of RITA data across the WAN, interview company personnel to determine what measures are in place to protect the circuits.	Expected Results: 1.Circuits are maintained on cable and not converted to unencrypted radio (microwave) transmission. The cable is protected by either being buried underground, or run through plenum area in walls, ceilings or floors. Access to cable and switching rooms is restricted. All wiring, conduits, and cabling are within the control of company personnel and that access to routers and network monitors are strictly controlled.		
84	Cryptographic Key Establishment and Management	Procedures: 1. Examine system and communications protection policy, procedures addressing cryptographic key management and establishment, information system design documentation; information system configuration settings and associated documentation and other relevant documents or records. (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.	1. The information system utilizes automated mechanisms with supporting procedures in place for digital certificate generation, installation, and distribution. Subscriber key pairs are generated and stored using FIPS 140-2 Security Level 2 or higher cryptographic modules. The same public/private key pair is not be used for both encryption and digital signature. Private keys are protected using, at a minimum, a strong password. A certificate is revoked if the associated private key is compromised; management requests revocation; or the certificate is no longer needed.		
85	Collaborative Computing	Procedures: 1. Examine the information system to verify whether or not it has collaborative computing mechanisms (Collaborative computing mechanisms include, for example, video and audio conferencing capabilities.). If the system does have collaborative computing mechanisms, then verify the ability to remotely execute those capabilities.	1. The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.		
86	Public Key Infrastructure Certificates	Procedures: 1. Examine system and communications protection policy, procedures addressing public key infrastructure certificates, public key certificate policy or policies, public key issuing process, and other relevant documents or records to determine if the company develops and implements a certificate policy and certification practice statement for the issuance of public key certificates at the company-wide level.	1. The company develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used at the company-wide level.		

ID	Control Name	Procedures	Expected Result	Actual Result	Status
87	Mobile Code	Procedures: 1. Examine system and communications protection policy, procedures addressing mobile code, mobile code usage restrictions, mobile code implementation guidance, and other relevant documents or records to determine if the company: 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 iii. requires company officials to approve the use of mobile code.	1. The company establishes usage restrictions and implementation guidance for mobile code technologies. Mobile code usage requires authorization and are documented and monitored. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript.		
88	Voice Over Internet Protocol	Procedures: 1. Examine applicable system and communications protection policy, procedures addressing VoIP, VoIP usage restrictions, and other relevant documents or records to determine if the company has established policies and guidance for the use of VoIP.	1. The company: (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, (iii) requires company officials to approve the use of VoIP.		
89	Electronic Mail	1. Examine company policy for handling RITA data and interview company personnel to determine if RITA data is transmitted via email. 2. If RITA data must be transmitted via email, examine company policy and interview company personnel to determine what measures are in place to secure RITA data during email transmission.	1. Company policy states RITA data shall not be transmitted or used on email systems. 2. If it is necessary to transmit RITA data via email, the following precautions must be taken to protect RITA data sent via email: • RITA approves the method used to protect RITA data being sent via email. • RITA data is encrypted in the email • Attachments containing RITA data are encrypted • Ensure that all messages sent are to the proper address, and • Employees should log off the computer when away from the area.		
90	Fax Machines	Procedures: 1. Examine company policy for handling RITA data and interview company personnel to determine if RITA data is transmitted via Fax machine.	1. If FAX machines are used to transmit RITA data the following security mechanisms are in place to protect Fax transmissions: • A trusted staff member is located at both the sending and receiving fax machines. • Broadcast lists and other preset numbers of frequent recipients of RITA data are maintained and periodically updated • Fax machines are placed in a secured area. • A cover sheet is included on fax transmissions that explicitly provides guidance to the recipient, which includes: - A notification of the sensitivity of the data and the need for protection - A notice to unintended recipients to telephone the sender—collect if necessary—to report the disclosure and confirm destruction of the information.		