TSA Registered Traveler

Appendix B:
Service Provider Self-Assessment Questionnaire

Version 3.1, January 2008

Transportation Security Administration

RT Registered Traveler™

Appendix B: Service Provider Self-Assessment Questionnaire

Service Provider Name: _____

Service Provider Address: _____

_____

_____

Date of Evaluation: _____

Service Provider Assertion

The [SERVICE PROVIDER NAME] management is responsible for establishing and maintaining effective security controls over [NAME OF RT APPLICATION/SYSTEM], which provides for the safeguarding of information assets and compliance with Registered Traveler Program requirements. The [SERVICE PROVIDER NAME] conducted its assessment of the effectiveness of the [NAME OF RT APPLICATION/SYSTEM] controls, including security controls, over [NAME OF RT APPLICATION/SYSTEM], in accordance with the modified National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26 Self Assessment and the Registered Traveler Program requirements.

Based on the results of this evaluation, the [SERVICE PROVIDER NAME] can provide reasonable assurance that the required controls applicable to [NAME OF RT APPLICATION/SYSTEM], as of [DATE], were operating effectively and no material weaknesses were found in the design or operation of these controls.

Corporate Officer:

_____
Signature Date

_____
Printed Name

Lead Assessor:

_____
Signature Date

_____
Printed Name

Sponsoring Entity Reviewer:

_____
Signature Date

_____
Printed Name

Registered Traveler Program Manager (if different from Lead Assessor):

_____
Signature Date

_____
Printed Name

Management Controls

Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.

1. Risk Management

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Risk Management	RA-1								
1.1 Critical Element: Is risk periodically assessed?									
1.1.1 Is the current system configuration documented, including links to other systems?	CM-2								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change?	RA-3 RA-4								
1.1.3 Has data sensitivity and integrity of the data been considered?	RA-2								
1.1.4 Have threat sources, both natural and manmade, been identified?	RA-3								
1.1.5 Has a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources been developed and maintained current?	RA-3								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
1.1.6 Has an analysis been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities?	RA-3								
1.2 Critical Element: Do program officials understand the risk to systems under their control and determine the acceptable level of risk?									
1.2.1 Are final risk determinations and related management approvals documented in the System Security Plan?	RA-3								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
1.2.3 Have additional controls been identified to sufficiently mitigate identified risks?	RA-3								

Notes:

2. Review of Security Controls

Routine evaluations and response to identified vulnerabilities are important elements of managing the risk of a system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Review of Security Controls									

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
2.1 Are security alerts and security incidents analyzed and remedial actions taken?	IR-4								

Notes:

3. Life Cycle

Like other aspects of an IT system, security is best managed if planned for throughout the IT system life cycle. There are many models for the IT system life cycle but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Life Cycle	SA-1								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.1 Critical Element: Has a system development life cycle method-ology been developed?									
Initiation Phase									
3.1.1 Is the sensitivity of the system deter-mined?	RA-2								
3.1.2 Are authorizations for software modifications documented and maintained?	CM-3								
Development/ Acquisition Phase									
3.1.3 During the system design, are security requirements identified?	SA-4								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.1.4 Was an initial risk assessment performed to determine security requirements?	RA-3 SA-4								
3.1.5 Is there a written agreement with system owners on the security controls employed and residual risk?	RA-3								
3.1.6 Are security controls consistent with and an integral part of the IT architecture?	CM-2								
Implementation Phase									

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.2 Critical Element: Are changes controlled as programs progress through testing to final approval?									
3.2.1 Are design reviews and system tests run prior to placing the system in production?	SA-8 SA-11								
3.2.2 Are the test results documented in the system security plan?	SA-8 SA-11								
3.2.3 Is verification and validation testing of security controls conducted and documented in the system security plan?	SA-5								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.2.4 If security controls were added since development, has the System Security Plan been modified to include them?	SA-5								
Operation/ Maintenance Phase									
3.2.5 Has a system security plan been developed and approved by the entity's management?	SA-5								
3.2.6 Is the system security plan kept current (updated yearly)?	PL-3								
Disposal Phase									
3.2.7 Are official electronic records properly disposed/ archived?	MP-6 MP-7								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.2.8 Is information or media purged, overwritten, degaussed, or destroyed when disposed or used elsewhere?	MP-6 MP-7								
3.2.9 Is a record kept of who implemented the disposal actions and verified that the information or media was sanitized?	MP-6 MP-7								

Notes:

4. Authorize Processing

Authorize processing (Note: Some agencies refer to this process as certification and accreditation) provides a form of assurance of the security of the system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Authorize Processing									
4.1 Critical Element: Has the system been certified/ recertified and authorized to process (accredited)?									
4.1.1 Has a risk assessment been conducted when a significant change occurred?	RA-4								
4.1.2 Have Rules of Behavior been established and signed by users?	PL-4								
4.1.3 Has a contingency plan been developed and tested?	CP-2 CP-4								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
4.1.4 Has a System Security Plan been developed, updated, and reviewed?	PL-2								
4.1.5 Are the planned and in-place controls consistent with the identified risks and the system and data sensitivity?	RA-3								

Notes:

5. System Security Plan

System security plans provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The plan delineates responsibilities and expected behavior of all individuals who access the system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
System security plan	PL-1								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
5.1 Critical Element: Is a system security plan documented for the system and all interconnected systems if the boundary controls are ineffective?									
5.1.1 Is the system security plan approved by key affected parties and management?	PL-2								
5.1.2 Does the plan contain the prescribed topics as outlined in Appendix E.	PL-2								
5.2 Critical Element: Is the plan kept current?									

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
5.2.1 Is the plan reviewed annually and adjusted to reflect current conditions and risks?	PL-3								

Notes:

Operational Controls

The operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls.

6. Personnel Security

Many important issues in computer security involve human users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Personnel Security	PS-1								

Specific Control Objectives	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
6.1 Critical Element: Are duties separated to ensure least privilege and individual accountability?									
6.1.1 Are all positions reviewed for sensitivity level?	AC-5 PS-2								
6.1.2 Are there documented job descriptions that accurately reflect assigned duties and responsi-bilities and that segregate duties?	AC-5 PS-2								
6.1.3 Are sensitive functions divided among different individuals?	AC-5								
6.1.4 Are distinct systems support functions performed by different individuals?	CM-5								

Specific Control Objectives	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
6.1.5 Are mechanisms in place for holding users responsible for their actions?	PS-6								
6.1.6 Are hiring, transfer, and termination procedures established?	PS-4 PS-5								
6.1.7 Is there a process for requesting, establishing, issuing, and closing user accounts?	AC-2								
6.2. Critical Element: Is appropriate background screening for assigned positions completed prior to granting access?									

Specific Control Objectives	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
6.2.1 Are individuals who are authorized to bypass significant technical and operational controls screened prior to access and periodically thereafter?	PS-3								
6.2.2 Are confidentiality or security agreements required for employees assigned to work with sensitive information?	PS-6								
6.2.3 When controls cannot adequately protect the information, are individuals screened prior to access?	PS-3								
6.2.4 Are there conditions for allowing system access prior to completion of screening?	PS-6								

Specific Control Objectives	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials

Notes:

7. Physical and Environmental Protection

Physical security and environmental security are the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Physical and Environmental Protection	PE-1								
Physical Access Control									

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.1 Critical Element: Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?									
7.1.1 Is access to facilities controlled through the use of guards, identification badges, or entry devices such as key cards or biometrics?	PE-2 PE-3								
7.1.2 Does management regularly review the list of persons with physical access to sensitive facilities?	PE-2 PE-3								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.1.3 Are keys or other access devices needed to enter the computer room and tape/media library?	MP-4								
7.1.4 Are unused keys or other entry devices secured?	PE-3								
7.1.5 Do emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after fire drills, etc?	PE-3								
7.1.6 Are visitors to sensitive areas signed in and escorted?	PE-7								
7.1.7 Are entry codes changed periodically?	PE-3								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.1.8 Is suspicious access activity investigated and appropriate action taken?	AC-13								
7.1.9 Are visitors, contractors and maintenance personnel authenticated through the use of preplanned appointments and identification checks?	PE-7								
Fire Safety Factors									
7.1.10 Are fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson, reviewed periodically?	RA-3								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.1.11 Have controls been implemented to mitigate other disasters, such as floods, earth-quakes, etc.?	RA-3								
Interception of Data									
7.2 Critical Element: Are mobile and portable systems protected?									
7.2.1 Are sensitive data files encrypted on all portable systems?	AC-19								
7.2.2 Are portable systems stored securely?	AC-19								

Notes:

8. Production, Input/Output Controls

There are many aspects to supporting IT operations. Topics range from a user help desk to procedures for storing, handling and destroying media. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Production, Input/Output Controls	MP-1								
8.1 Critical Element: Is there user support?									
8.1.1 Is there a help desk or group that offers advice?	IR-7								
8.2 Critical Element: Are there media controls?									
8.2.1 Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?	MP-2 MP-4								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
8.2.2 Are there processes for ensuring that only authorized users pick up, receive, or deliver input and output information and media?	MP-2 MP-4 MP-5								
8.2.3 Are audit trails used for receipt of sensitive inputs/ outputs?	MP-2								
8.2.4 Is there internal/external labeling for sensitivity?	MP-3								
8.2.5 Is there external labeling with special handling instructions?	MP-2 MP-3								
8.2.6 Are audit trails kept for inventory management?	MP-2								
8.2.7 Is media sanitized for reuse?	MP-6								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
8.2.8 Is damaged media stored and /or destroyed?	MP-4 MP-6								
8.2.9 Is hardcopy media shredded or destroyed when no longer needed?	MP-7								

Notes:

9. Contingency Planning

Contingency planning involves more than planning for a move offsite after a disaster destroys a facility. It also addresses how to keep an organization's critical functions operating in the event of disruptions, large and small. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Contingency Planning	CP-1								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
9.1 Critical Element: Have the most critical and sensitive operations and their supporting computer resources been identified?									
9.1.1 Are critical data files and operations identified and the frequency of file backup documented?	CP-2 CP-9								
9.1.2 Are resources supporting critical operations identified?	MA-6								
9.1.3 Have processing priorities been established and approved by management?	CP-7								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
9.2 Critical Element: Has a comprehensive contingency plan been developed and documented?									
9.2.1 Is the plan approved by key affected parties?	CP-2								
9.2.2 Are responsibilities for recovery assigned?	CP-2								
9.2.3 Are there detailed instructions for restoring operations?	CP-2								
9.2.4 Is there an alternate processing site; if so, is there a contract or interentity agreement in place?	CP-6 CP-7								
9.2.5 Is the location of stored backups identified?	CP-6 CP-7								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
9.2.6 Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged?	CP-9								
9.2.7 Is system and application documentation maintained at the off-site location?	CP-6 CP-7								
9.2.8 Are all system defaults reset after being restored from a backup?	CP-10								
9.2.9 Are the backup storage site and alternate site geographi-cally removed from the primary site and physically protected?	CP-6 CP-7 CP-9								
9.2.10 Has the contingency plan been distributed to all appropriate personnel?	CP-2								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
9.3 Critical Element: Are tested contingency/ disaster recovery plans in place?									
9.3.1 Is an up-to-date copy of the plan stored securely off-site?	CP-5 CP-9								
9.3.2 Are employees trained in their roles and responsibilities?	CP-3								
9.3.3 Is the plan periodically tested and readjusted as appropriate?	CP-4 CP-5								

NOTES:

10. Hardware and System Software Maintenance

These are controls used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of changes. Some of these controls are also covered in the Life Cycle Section. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Hardware and System Software Maintenance	MA-1								
10.1 Critical Element: Is access limited to system software and hardware?									
10.1.1 Are restrictions in place on who performs maintenance and repair activities?	CM-5 MA-2 MA-4 MA-5								
10.1.2 Is access to all program libraries restricted and controlled?	AC-3 MP-4								
10.1.3 Are there on-site and off-site maintenance procedures (e.g., escort of maintenance personnel, sanitization of devices removed from the site)?	MA-2 MA-3 MA-5								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.1.4 Is the operating system configured to prevent circumvention of the security software and application controls?	CM-5								
10.1.5 Are up-to-date procedures in place for using and monitoring use of system utilities?	CM-5								
10.2 Critical Element: Are all new and revised hardware and software authorized, tested and approved before implementation?									

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.2.1 Is an impact analysis conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control?	CM-4 MA-2								
10.2.2 Are system components tested, documented, and approved (operating system, utility, applications) prior to promotion to production?	CM-3								
10.2.3 Are software change request forms used to document requests and related approvals?	CM-3								
10.2.4 Are there detailed system specifications prepared and reviewed by management?	CM-4								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.2.5 Is the type of test data to be used specified, i.e., live or made up?	SA-11								
10.2.6 Are default settings of security features set to the most restrictive mode?	CM-6								
10.2.7 Are there software distribution implementation orders including effective date provided to all locations?	CM-2								
10.2.8 Is there version control?	CM-3								
10.2.9 Are programs labeled and inventoried?	CM-2 MP-3								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.2.10 Are the distribution and implementation of new or revised software documented and reviewed?	CM-3 SA-6 SA-7								
10.2.11 Are emergency change procedures documented and approved by management, either prior to the change or after the fact?	CM-3								
10.2.12 Are contingency plans and other associated documentation updated to reflect system changes?	CP-5								
10.2.13 Is the use of copyrighted software or shareware and personally owned software/ equipment documented?	AC-20 SA-6								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.3. Are systems managed to reduce vulnerabilities?									
10.3.1 Are systems periodically reviewed to identify and, when possible, eliminate unnecessary services (e.g., FTP, HTTP, mainframe supervisor calls)?	CM-6 CM-7								
10.3.2 Are systems periodically reviewed for known vulnerabilities and software patches promptly installed?	RA-5 SI-2								

NOTES:

11. Data Integrity

Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user the information meets expectations about its quality and integrity. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Data Integrity	SI-1								
11.1 Critical Element: Is virus detection and elimination software installed and activated?									
11.1.1 Are virus signature files routinely updated?	SI-2 SI-3								
11.1.2 Are virus scans automatic?	SI-2								
11.2 Critical Element: Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?	SI-3								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
11.2.1 Are reconciliation routines used by applications, i.e., checksums, hash totals, record counts?	SC-8 SI-6 SI-7								
11.2.2 Is inappropriate or unusual activity reported, investigated, and appropriate actions taken?	AC-13 SI-2 SI-6								
11.2.3 Are procedures in place to determine compliance with password policies?	IA-1								
11.2.4 Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions?	SC-8 SI-7 MA-3								
11.2.5 Are intrusion detection tools installed on the system?	SI-4								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
11.2.6 Are the intrusion detection reports routinely reviewed and suspected incidents handled accordingly?	SI-4								
11.2.7 Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks?	SI-2								
11.2.8 Is message authentication used?	SC-8								

NOTES:

12. Documentation

The documentation contains descriptions of the hardware, software, policies, standards, procedures, and approvals related to the system and formalize the system's security controls. When answering whether there are procedures for each control objective, the question should be phrased "are there procedures for ensuring the documentation is obtained and maintained." The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Documentation									
12.1 Critical Element: Is there sufficient documentation that explains how software/ hardware is to be used?									
12.1.1 Is there vendor-supplied documentation of purchased software?	SA-5								
12.1.2 Is there vendor-supplied documentation of purchased hardware?	SA-5								
12.1.3 Is there application documentation for in-house applications?	SA-5								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
12.1.4 Are there network diagrams and documentation on setups of routers and switches?	AC-8 CM-2								
12.1.5 Are there software and hardware testing procedures and results?	SA-11								
12.1.6 Are there standard operating procedures for all the topic areas covered in this document?	SA-5								
12.1.7 Are there user manuals?	SA-5								
12.1.8 Are there emergency procedures?	CP-2								
12.1.9 Are there backup procedures?	CP-9								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
12.2 Critical Element: Are there formal security and operational procedures documented?									
12.2.1 Is there a system security plan?	PL-2								
12.2.2 Is there a contingency plan?	CP-2								
12.2.3 Are there written agreements regarding how data is shared between interconnected systems?	SA-9								
12.2.4 Are there risk assessment reports?	RA-3								

NOTES:

13. Security Awareness, Training, and Education

People are a crucial factor in ensuring the security of computer systems and valuable information resources. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge. The following questions are organized according to one critical element. The levels for the critical element should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Security Awareness, Training, and Education	AT-1								
13.1 Critical Element: Have employees received adequate training to fulfill their security responsibil-ities?									
13.1.1 Have employees received a copy of the Rules of Behavior?	PL-4								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
13.1.2 Are employee training and professional development documented and monitored?	AT-4								
13.1.3 Is there mandatory annual refresher training?	AT-3								
13.1.4 Are methods employed to make employees aware of security, i.e., posters, booklets?	AT-2								
13.1.5 Have employees received a copy of or have easy access to entity security procedures and policies?	AT-2 AT-3								

NOTES:

14. Incident Response Capability

Computer security incidents are an adverse event in a computer system or network. Such incidents are becoming more common and their impact far-reaching. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Incident Response Capability	IR-1								
14.1 Critical Element: Is there a capability to provide help to users when a security incident occurs in the system?									
14.1.1 Is a formal incident response capability available?	IR-4 IR-7 SI-5								
14.1.2 Is there a process for reporting incidents that is compliant with the incident reporting requirements set forth in the RT Standards?	IR-4 IR-6 SI-5								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
14.1.3 Are incidents monitored and tracked until resolved?	IR-5 IR-6								
14.1.4 Are personnel trained to recognize and handle incidents?	IR-2								
14.1.5 Are alerts/advisories received and responded to?	SI-5								
14.1.6 Is there a process to modify incident handling procedures and control techniques after an incident occurs?	IR-4								
14.2 Critical Element: Is incident related information shared with appropriate organizations?									

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
14.2.1 Is incident information and common vulnerabilities or threats shared with owners of interconnected systems?	IR-6 RA-5								
14.2.3 Is incident information reported to local law enforcement when necessary?	IR-6								

NOTES:

Technical Controls

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

15. Identification and Authentication

Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Identification and Authentication	AC-1 IA-1								
15.1 Critical Element: Are users individually authenticated via passwords, tokens, or other devices?									
15.1.1 Is a current list maintained and approved of authorized users and their access?	AC-2 AC-3 IA-4								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
15.1.2 Are digital signatures used and conform to the RTIC Technical Interoperability Specification?	AU-10								
15.1.3 Are access scripts with embedded passwords prohibited?	IA-2								
15.1.4 Is emergency and temporary access authorized?	AC-2								
15.1.5 Are personnel files matched with user accounts to ensure that terminated or transferred individuals do not retain system access?	AC-2								
15.1.6 Are passwords changed at least every ninety days or earlier if needed?	IA-5								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
15.1.7 Are passwords unique and difficult to guess (e.g., do passwords require alpha numeric, upper/lower case, and special characters)?	IA-5								
15.1.8 Are inactive user identifications disabled after a specified period of time?	AC-2 IA-4								
15.1.9 Are passwords not displayed when entered?	IA-5								
15.1.10 Are there procedures in place for handling lost and compromised passwords?	IA-5								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
15.1.11 Are passwords distributed securely and uses informed not to reveal their passwords to anyone (social engineering)?	IA-5								
15.1.12 Are passwords transmitted and stored using secure protocols/ algorithms?	IA-5								
15.1.13 Are vendor-supplied passwords replaced immedi-ately?	IA-5								
15.1.14 Is there a limit to the number of invalid access attempts that may occur for a given user?	AC-7								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
15.2 Critical Element: Are access controls enforcing segregation of duties?									
15.2.1 Does the system correlate actions to users?	AC-5								
15.2.2 Do data owners periodically review access authorizations to determine whether they remain appropriate?	AC-2 IA-4								

NOTES:

16. Logical Access Controls

Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Logical Access Controls	AC-1								
16.1 Critical Element: Do the logical access controls restrict users to authorized transactions and functions?									
16.1.1 Can the security controls detect unauthorized access attempts?	AC-3								
16.1.2 Is there access control software that prevents an individual from having all necessary authority or information access to allow fraudulent activity without collusion?	AC-3 AC-5 AC-6								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.1.3 Is access to security software restricted to security administrators?	AC-2 AC-3 AC-6 IA-5								
16.1.4 Do workstations disconnect or screen savers lock system after a specific period of inactivity?	AC-11 AC-12								
16.1.5 Are inactive users' accounts monitored and removed when not needed?	AC-2								
16.1.6 If encryption is used, does it meet RT Standards for data at rest and transmission?	AC-3 IA-7 SC-12 SC-13								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.1.7 If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving?	SC-12 SC-13								
16.1.8 Is access restricted to files at the logical view or field?	AC-3								
16.1.9 Is access monitored to identify apparent security violations, and are such events investigated?	AC-13								
16.2 Critical Element: Are there logical controls over network access?									
16.2.1 Has communication software been implemented to restrict access through specific terminals?	AC-3								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.2.2 Are insecure protocols (e.g., UDP, ftp) disabled?	CM-6 SC-7								
16.2.3 Have all vendor-supplied default security parameters been reinitialized to more secure settings?	CM-6 IA-5								
16.2.4 Are there controls that restrict remote access to the system?	AC-17								
16.2.5 Are network activity logs maintained and reviewed?	AC-13 AU-6								
16.2.6 Does the network connection automatically disconnect at the end of a session?	AC-12 SC-10								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.2.7 Are trust relationships among hosts and external entities appropriately restricted?	AC-3 IA-3 SC-7 SC-11								
16.2.8 Is dial-in access monitored?	AC-17								
16.2.9 Are firewalls or secure gateways installed?	AC-3 SC-7								
16.2.10 If firewalls are installed do they comply with firewall policy and rules?	AC-3 CM-6 SC-7								
16.2.11 Are guest and anonymous accounts authorized and monitored?	AC-2 AC-14								
16.2.12 Are sensitive data transmissions encrypted using the Advanced Encryption Standard?	SC-7 SC-8								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.2.13 Is access to tables defining network options, resources, and operator profiles restricted?	AC-3								
16.3 Critical Element: If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?									
16.3.1 Is a privacy policy posted on the web site and is the policy consistent with Privacy Act requirements?	AC-8								

NOTES:

17. Audit Trails

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems. The following questions are organized under one critical element. The levels for the critical element should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Audit Trails	AU-1								
17.1 Critical Element: Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?									
17.1.1 Does the audit trail provide a trace of user actions?	AU-2 AU-3 AU-10								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
17.1.2 Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased?	AU-2 AU-7								
17.1.3 Is access to online audit logs strictly controlled?	AU-9								
17.1.4 Are off-line storage of audit logs retained for a period of time, and if so, is access to audit logs strictly controlled?	AU-2 AU-9 AU-11								
17.1.5 Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?	AC-5 AC-6								

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
17.1.6 Are audit trails reviewed frequently?	AC-13								
17.1.7 Are automated tools used to review audit records in real time or near real time?	AC-13 AU-6 AU-7								
17.1.8 Is suspicious activity investigated and appropriate action taken?	AU-6								
17.1.9 Is keystroke monitoring used? If so, are users notified?	AC-8								

NOTES:

18. Enrollment Process

The Enrollment Process is compromised of four major processes: biographic information collection, document validation, biometric collection, and card production and issuance. The following questions are organized under four critical elements. The level for the critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Enrollment Process								
18.1 Critical Element: Biographic Information Collection								
18.1.1 Do EP kiosks adhere to physical security controls to prevent individuals from compromising Personally Identifiable Information (PII)?								
18.1.2 Does surveillance around the kiosk record unauthorized acquisition of PII?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
18.1.3 Do all public facing websites have a valid Secure Socket Link (SSL) certificate issued by an authorized certificate vendor e.g. Thwart or Verisign that is current and complies with the RT encryption standards?								
18.1.4 Do 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?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
18.1.5 Do audit trails exist to uniquely identify EP personnel who verify the accuracy of the biographic data and the validation of personal identification documents?								
18.1.6 Are EP systems designed with field edits to detect inappropriate entries?								
18.1.7 Do systems controls exist which require dual validation of personal identification documents?								
18.2 Document Validation								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
18.2.1 Do EPs utilize document authentication technologies that take advantage of anti-fraud features incorporated into government-issued documents?								
18.2.2 Are policies and procedures in place to ensure EP personnel are appropriately trained to utilize validation devices and recognize counterfeit personal identification documents?								
18.3 Biometric Collection								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
18.3.1 Do system access controls exist which require the separation of duties between the authorization of biographic data and the collection of biometrics?								
18.3.2 Are procedures 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?								
18.3.3 Do audit trails exist to uniquely identify EP personnel who collect biometric data?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
18.3.4 Are policies and procedures in place to ensure EP personnel are appropriately trained to assist in the collection of RT Applicant biometrics in accordance with CIMS specifications? (Are records kept to verify training has been completed?)								
18.3.5 Are systematic controls in place to ensure biometric are captured in accordance with CIMS specifications?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
18.3.6 Do EP personnel biometrically authenticate themselves as they complete each enrollment package? Does the enrollment workstation have the capability to record EP traceability in such that each completed transaction can be tracked back to them?								
18.3.7 Are systematic controls in place to ensure biometrics are captured in accordance with the RTIC Technical Interoperability Specification?								
18.4 Card Production and Issuance								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
18.4.1 Do EP systems have the ability to modify the payload data on the RT Card.								
18.4.2 Do RT cards have a read only mode (once the information is created it can only be read/not altered)?								
18.4.3 Is unauthorized viewing of the card information prevented?								
18.4.4 Are RT cards only issued upon receipt of an approved security threat assessment for each individual?								
18.4.5 Are RT cards are only replaced as necessary and reported to CIMS?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
18.5 Data Collection & Storage								
18.5.1 Are archived electronic copies of enrollment forms maintained in accordance with the SP's written privacy policy?								
18.6 Excess Data								
18.6.1 Does the entity collect excess data in accordance with the RT Standards?								
18.6.2 Is there a logical separation between RT required data and excess data?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
18.7 Information Provided To and Received From Applicant								
18.7.1 Is the RT required information provided to all applicants?								
18.8 Enrollment Conformance								
18.8.1 Has the entity passed CIMS conformance testing for providing enrollment services?								

NOTES:

19. Verification Process

The Verification Process is compromised of two major processes: checkpoint verification and metrics. The following questions are organized under five critical elements. The levels for the critical element should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Verification Process								
19.1 Checkpoint Verification								
19.1.1 Is the physical chain of custody 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?								
19.1.2 Does the VP ensure that the required traveler identity verification procedures are performed in accordance with applicable TSA regulations and procedures?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
19.1.3 Is the unique identifier 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?								
19.1.4 Do VPs ensure employees have undergone Criminal History Records Checks (CHRC) and Security Threat Assessments (STA), conduct ethics training, and provide for surveillance over manned kiosks?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
19.1.5 Do Verification Personnel biometrically authenticate themselves upon accessing the kiosk? Does the verification kiosk have the capability to record Verification Personnel traceability in such that each RT participation authentication can be tracked back to them?								
19.2 Verification Controls								
19.2.1 Do VPs ensure there is a maximum number of biometric attempts before the RT Participant is rejected from the kiosk?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
19.2.2 Do the cards contain the phrase: "This is not a government identification card?"								
19.2.3 Do the cards contain photo representation and full legal name of RT participant?								
19.3 Metrics								
19.3.1 Do VP systems maintain sufficient metrics to measure false rejection rates?								
19.3.2 Do VPs monitor false acceptance and rejection rates on a daily basis?								
19.3.3 Do VPs collect metrics as specified in Section 4 of the RT Standards?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
19.4 Verification Conformance								
19.4.1 Has the entity passed CIMS conformance testing for providing verification services?								

NOTES:

20. Privacy

Privacy controls pertain to the mechanisms and processes used to protect personal information. The following questions are organized under 10 critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Privacy								
20.1 Openness								
20.1.1 Is the privacy policy documented?								
20.1.2 Does the privacy policy define and assign responsibilities for implementation?								
20.1.3 Is the privacy policy communicated to internal personnel?								
20.2 Collection Limitation								
20.2.1 Does the organization collect personal information only for the purposes identified in the notice?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
20.2.2 Does the organization provide the choices available to RT applicants in their privacy notice?								
20.2.3 Does the notice require explicit consent from RT applicants with respect to the collection, use, and disclosure of personal information?								
20.2.4 Are RT applicants informed of the consequences of refusing to provide personal information or of denying or withdrawing consent to use personal information for purposes identified in the notice?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
20.3 Purpose Specification								
20.3.1 Does the organization provide RT applicants notice of how their personal information is collected, used, retained and disclosed?								
20.3.2 Is the privacy notice conspicuous and use clear language?								
20.3.3 Does the entity provide all applicants with the TSA Privacy Act Statement at the time of enrollment?								
20.4 Use Limitation								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
20.4.1 Does the organization limit the use of personal information to the purpose identified in the privacy notice?								
20.4.2 Does the organization limit the use of personal information to where the individual has provided consent?								
20.5 Data Quality								
20.5.1 Does the organization maintain accurate, complete, and relevant personal information for the purposes identified in the notice?								
20.6 Individual Participation								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
20.6.1 Does the organization provide individuals with access to review and update their personal information?								
20.6.2 Does the organization authenticate individuals before granting them access to their personal information?								
20.6.3 Does the organization have procedures to address privacy-related complaints and disputes?								
20.7 Security Safeguards								
20.7.1 Does the organization ensure that security measures are in place to protect privacy information?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
20.8 Accountability								
20.8.1 Does the organization monitor compliance with its privacy policies and procedures?								

NOTES:

21. Registered Traveler Controls

RT controls pertain to the mechanisms and processes used to protect RT information. The following questions are organized under 7 critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions..

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
RT Controls								
21.1 Equal Access								
21.1.1 Does the entity provide equal access to all RT applicants?								
21.2 Security Status								
21.2.1 Does the entity transmit employee information to TSA as required for key personnel?								
21.2.2 Does the entity process daily updates to card revocation lists as provided by the CIMS?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
21.3 Updates to Biometric Information								
21.3.1 Does the entity re-verify identity documents and recapture digital images whenever an RT Participant reports changes or updates to their personal information?								
21.4 RT Card Deactivation								
21.4.1 Is a policy in place for the entity to notify CIMS within 24 hours when a card should be deactivated?								
21.5 Interoperability								
21.5.1 Does the entity accept RT Participants from all approved SPs?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
21.5.2 Does the entity provide access to RT lines at no additional cost to the RT Participant?								
21.6 Approval to Operate								
21.6.1 Has the entity contracted with an IPA firm to perform an annual attestation of compliance with the RT Standards and required controls?								
21.6.2 Did the entity obtain an attestation report and TSA approval before commencing operations?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
21.7 Oversight								
21.7.1 Does the entity have a provision in its contract with the SE that allows for TSA oversight of RT operations?								
21.7.2 Does the entity have a provision in its contract with the SE that allows for TSA to audit or inspect the controls over the SP's RT Program?								

NOTES:

Homeland Security

RT Registered Traveler™