

# Transportation Security Administration

## Registered Traveler Model

May 2006

### Table of Contents

<b>1. Introduction.....</b>	<b>1</b>
1.1 Purpose .....	1
1.2 Registered Traveler Concept.....	1
1.3 Next Steps .....	2
1.4 Key Players.....	2
1.5 Overview .....	3
1.6 Sponsoring Entity Participation.....	7
1.7 Relationship to Other Programs .....	8
<b>2. Eligibility.....</b>	<b>8</b>
2.1 Population.....	8
2.2 Disposition of Minors .....	8
2.3 Other .....	8
<b>3. Functional Elements of the RT Program.....</b>	<b>9</b>
3.1 Introduction .....	9
3.2 Pre-enrollment .....	10
3.3 Enrollment.....	11
3.3.1. Documents.....	11
3.3.2. Biographic Data .....	11
3.3.3. Biometric Data .....	12
3.3.4. Privacy.....	13
3.4 Central Information Management System.....	14
3.4.1. Transmittal.....	14
3.4.2. Duplicate Check.....	14
3.5 Security Threat Assessment.....	14
3.6 Card Production and Issuance .....	15
3.7 Program Fees and Membership Renewal.....	16
3.8 Verification and Use.....	17
3.9 Credential Revocation List.....	18
3.10 Standards and Conformance.....	18
<b>4. Security Procedures and Benefits.....</b>	<b>19</b>
4.1 RT Screening Procedures and Security Related Benefits .....	19
4.2 Ancillary (non-security) Benefits .....	19
<b>5. Data Transfer and Storage Model .....</b>	<b>20</b>

## **1. Introduction**

### **1.1 Purpose**

The following Registered Traveler Model is meant to provide stakeholders and interested members of the general public with a basis for discussing and planning for Registered Traveler (RT). RT will launch as a partnership among airports, air carriers, industry, and TSA. The agency intends to proceed with RT through an initial phase at airports in the second half of 2006, to be followed by a national program implemented through the Federal rulemaking process.

This document is not meant to represent the final product in RT's development, but rather a snapshot of the current concept of the program's structure. This RT Model discusses RT as it is broadly envisioned for the initial phase and, consequently, does not include all possibilities for future enhancements. With the release of this model, the Transportation Security Administration (TSA) intends to stimulate the consultative process as RT evolves.

TSA will issue standards for the operation of RT by the airports, air carriers and industry Service Providers. This RT Model will be used in the development of those standards but should not be considered a substitute for them. In cases where the standards or other governing documents conflict with the information in this RT Model, the standards or other governing documents shall take precedence.

TSA invites comments and suggestions on this RT Model. While TSA cannot guarantee that all submissions will receive a response, submissions will be reviewed and the RT Model amended as appropriate. Comments may be submitted to TSA electronically through the following e-mail address: [Registered.Traveler@dhs.gov](mailto:Registered.Traveler@dhs.gov). Written comments may be submitted to TSA at the following address: Registered Traveler Program, Office of Transportation Threat Assessment and Credentialing (TTAC), TSA-19, Transportation Security Administration, 601 South 12th Street, Arlington, VA 22202-4220.

### **1.2 Registered Traveler Concept**

The RT concept is authorized under the Aviation and Transportation Security Act (ATSA) as a means to "establish requirements to implement trusted passenger programs and use available technologies to expedite security screening of passengers who participate in such programs." TSA will facilitate a partnership with the private sector to establish an interoperable, vendor-neutral RT program in the United States. RT potentially offers many potential advantages for the TSA, industry, and the traveling public through enhanced security and customer service.

An interoperable, nationwide RT program depends on the implementation of a technical, operational, and business model capable of supporting the needs of individual airports, while providing the common infrastructure that allows passengers to use this capability at any participating airport. As a result, TSA requires a common set of business processes and technical standards necessary for an open, secure and industry-driven network that will create a fair and seamless platform for airports, airlines and vendors to interface with TSA and each other. Rather than preordaining any one proprietary system, this open-architecture approach ensures that

airports have an opportunity to work with any number of vendors to design a system that works best at their facilities. This approach also ensures that the creativity and competitive forces of the private sector are given the opportunity to serve local needs and keep program costs in check. Currently the private industry is working within the RTIC to recommend open technical standards. TSA encourages stakeholders to participate in this effort.

In developing the RT concept, TSA actively solicited the private sector to receive inputs on the required business practices and technical interoperability standards. In December 2005, a Request for Information (RFI) was published and an Industry Day was held at TSA headquarters to describe the objectives of the program and solicit ideas on the implementation of a nationwide program. TSA received and reviewed 75 responses from the private sector and incorporated them into this model as appropriate.

### 1.3 Next Steps

TSA will follow the release of the RT Model by issuing RT standards for the initial phase during the summer of 2006 and begin the rulemaking process for the national program later in the year. The RT design will evolve throughout the coming year, incorporating lessons learned and best practices throughout the process.

TSA expects to issue draft RT standards for the initial phase in or around June 2006, developed in conjunction with competitively-awarded contractor support, to detail the standards for Service Providers and Sponsoring Entities and govern the execution of their responsibilities in RT. These RT standards will describe the operations, personnel security, information technology, privacy, and other such standards. It will provide a common baseline for participation in RT by the private sector to ensure security needs are met and are continually validated. The standards will provide definition and detail to many of the elements discussed broadly in the RT Model.

TSA intends to begin the NPRM process on the national program this year. The rulemaking process is the regulatory development process proscribed through law and Department and Administration requirements. It is designed to ensure that the public has full opportunity to review the construct of a national RT program and influence the outcome through providing formal comments. The RT rulemaking will involve: 1) Development of a Notice of Proposed Rulemaking (NPRM) and any required supporting analyses; 2) Publication of NPRM; 3) Public comment period; 4) Analysis and disposition of comments through a Final Rulemaking, as appropriate; and 5) Publication of Final Rule.

### 1.4 Key Players

**Central Information Management System (CIMS):** A system to aggregate, store and distribute information (on an as needed basis) to the entities participating in RT. Responsibilities include: Receiving, aggregating, and formatting RT Applicant data from Enrollment Providers; Performing checks to identify potential duplicate enrollments to ensure application integrity; Transmitting applicant data to TSA for the agency to conduct Security Threat Assessments (STAs) (e.g., checks against Government databases to determine eligibility for RT); Receiving the determination of eligibility from TSA; Maintaining and distributing the Credential Revocation

list (consisting of unique identifiers); and Generating the biometric payload and encryption protocols for RT cards.

**Enrollment Provider (EP):** An RT Service Provider that collects the biographical and biometric information from RT Applicants, collects user fees from RT Applicants, and issues RT cards to RT participants. An Enrollment Provider may be the same entity as a Verification Provider.

**RT Applicant:** An individual who has voluntarily supplied biographical and biometric data to an RT Enrollment Provider with the intent of joining RT and paying the associated user fee.

**RT Participant:** An individual who has voluntarily enrolled with an Enrollment Provider, receives and maintains an approved STA from TSA, and meets all other requirements set by TSA. Commonly referred to as an “RT” or “Registered Traveler.”

**Service Providers:** A term of collective reference for Verification Providers and for Enrollment Providers. References in this RT Model to the Service Providers’ responsibilities do not relieve the Sponsoring Entities of accountability for assuring that the Service Providers’ activities comply with TSA-set standards.

**Sponsoring Entity:** An airport or air carrier, subject to TSA regulations, that manages the RT program at a particular site or sites. These entities select and qualify all participating Service Providers in accordance with TSA standards.

**Transportation Security Officer (TSO):** Formerly known as Screeners, TSOs are the TSA personnel who operate the airport security checkpoint and conduct security screening of all persons entering the sterile area.

**Transportation Security Administration (TSA):** The Transportation Security Administration, the Department of Homeland Security, or any successor Federal Government entity. Responsible for STAs, establishing qualification of RT Service Providers and regulatory oversight of the RT program.

**Verification Provider (VP):** RT Service Provider that verifies the identity of the RT Participant in the airport in accordance with TSA-issued RT standards; may be the same entity as an Enrollment Provider.

## **1.5 Overview**

Registered Traveler will be a private sector program, supported and regulated by TSA, with distinct roles and responsibilities for each participating entity. Table 1 describes the basic responsibilities of each entity.

Table 1

Participating Entity	Responsibilities
Enrollment Provider	<ul style="list-style-type: none"> <li>▪ Pre-enrollment</li> <li>▪ Biographic information collection</li> <li>▪ Biometric collection</li> <li>▪ Document validation</li> <li>▪ Card production and issuance</li> <li>▪ Card re-issuance</li> <li>▪ User fee collection</li> <li>▪ Customer service</li> </ul>
Verification Provider	<ul style="list-style-type: none"> <li>▪ Checkpoint investment (technology and personnel)</li> <li>▪ Checkpoint verification</li> <li>▪ Metrics collection</li> </ul>
Sponsoring Entity (Airports, Air Carriers, Consortium)	<ul style="list-style-type: none"> <li>▪ Selection of Service Providers</li> <li>▪ Qualification of sponsored Service Providers</li> <li>▪ Audit of sponsored verification providers</li> <li>▪ Checkpoint configuration coordination</li> </ul>
Central Information Management System (CIMS) and Financial Management System	<ul style="list-style-type: none"> <li>▪ Collection of enrollment information</li> <li>▪ Storage of biometrics</li> <li>▪ Format and pass through of data required for TSA vetting</li> <li>▪ Maintenance of participant and revocation databases</li> <li>▪ PKI/certification management</li> <li>▪ Card payload creation</li> <li>▪ Fee pass through to TSA</li> <li>▪ Interoperability testing</li> </ul>
TSA	<ul style="list-style-type: none"> <li>▪ Security screening processes</li> <li>▪ Security screening benefits</li> <li>▪ Security threat assessment</li> <li>▪ Checkpoint technology certification</li> <li>▪ Establish security standards</li> <li>▪ Establish audit criteria</li> <li>▪ Auditing of Service Providers</li> <li>▪ Redress and appeals</li> </ul>

Airports and air carriers will be the Sponsoring Entities that contract with RT Service Providers through their own acquisition processes. They may act individually or form consortiums to present proposals on behalf of individual airports and/or air carriers, but consortiums may not serve as Sponsoring Entities. These entities may choose comprehensive Service Providers, which provide a complete solution with all the functionalities associated with Service Providers, including enrollment, issuance and verification, or they may choose separate Service Providers for each essential function. Each Sponsoring Entity will have the discretion to select the service model most appropriate for its particular operation.

In the case of Enrollment Providers, the Sponsoring Entities will be responsible for selecting and coordinating enrollment sites. Any Sponsoring Entity that is not an airport or leaseholder will be required to coordinate with airports and TSA on the location of verification sites in proximity to the RT checkpoint lanes.

The Sponsoring Entities will be responsible for all costs associated with adding new passenger screening lanes or rededicating existing lanes<sup>1</sup> for RT purposes, as well as the staffing and maintenance of these lanes. In the case where an RT lane is a rededication of existing resources, the Service Provider will reimburse TSA for TSOs and associated costs at an hourly rate to be established as part of the RT fees which TSA will set by notice in the Federal Register.<sup>2</sup> Requests for additional lanes are subject to airport and TSA approval based on the unique operational set-ups of the individual airports and their checkpoints. TSA-approved checkpoint equipment for new RT lanes can be purchased by the Service Provider or Sponsoring Entity, depending on the physical constraints of the respective location. Additional screening personnel will be managed by TSA, which will be reimbursed by the Sponsoring Entity as part of the RT fees established by TSA through notice in the Federal Register.

Airports manned with TSOs may not hire contract screeners for RT lanes, and airports manned with contract screeners may not hire TSOs for RT lanes.

The Sponsoring Entity will conduct oversight of its Service Providers, which will also be subject to oversight by TSA in accordance with TSA-issued RT standards. TSA-issued standards for performance will become part of the Sponsoring Entity's Airport Security Plan (ASP) or Aircraft Operator Standard Security Plan (AOSSP) through TSA-approved amendments. The agreements between TSA and the Sponsoring Entities will use standardized language that address common operational issues but will also have the adaptability to fit the needs of each local airport environment.

TSA expects that one of the standards with which Service Providers will be required to comply is a condition to allow TSA or its contractors to conduct audits or inspections. If a Sponsor's Service Providers do not meet the standards contained in the ASP or AOSSP, TSA will notify and work with the Sponsoring Entity to bring element into compliance. The Sponsoring Entity is responsible for its Service Providers being in compliance and is subject to enforcement action by

---

<sup>1</sup> Rededication may occur where RT volumes are at a level sufficient not to negatively impact the non-RT travelers.

<sup>2</sup> The Sponsoring Entity may hold a Service Provider accountable for these costs based on the terms of the applicable procurement documents.

TSA, including, in extreme circumstances, suspension or withdrawal of authorization to participate in RT.

Verification Providers will conduct operations at a particular airport or at a TSA-approved offsite checkpoint in accordance with the standards to be established by TSA. Enrollment Providers may conduct operations at any location in a manner consistent with RT standards and are not restricted by TSA in where they may market their services.

TSA will require that all Service Providers participating in RT are both interoperable and belong to the Central Information Management System (CIMS) network. The CIMS will be a commercially neutral entity meant to support an open market place. A combination of Memorandum of Understanding (MOU) and Interface Control Documents will govern the relationships among the CIMS and the different Services Providers. The interoperability of any particular Service Provider will be verified by the CIMS before TSA gives final approval for participation. Interoperability will be based on open technical standards recommended by private industry and approved by TSA. All airports and air carriers that choose to participate will be able to participate as long as they are able to meet all standards set by TSA.

Sponsoring Entities and Service Providers will be responsible for resolving all industry-related liability issues associated with the program. While not mandated, RT Service Providers may apply for designation or certification under the U.S. SAFETY Act, which is designed to provide certain protections in the event of terrorist incidents.

Each Sponsoring Entity participating in the program will have a TSA-approved ASP or AOSSP amendment that will describe the operation of enrollment and verification functions at individual airports. These documents will contain the operational and technical standards required to ensure the security of the RT process and the protection of participants' privacy as specified, as a minimum standard, by TSA.

All Service Providers conducting enrollment will be required to submit a fee per applicant enrollment (and per RT Participant renewal), through the Financial Management System (FMS) component of the CIMS, to TSA to cover the agency's costs. This fee will be established by the Secretary of Homeland Security through publication of a notice in the Federal Register. The fee will be a flat amount paid initially at enrollment and on an annual per participant renewal basis to cover all TSA costs. This fee will be non-refundable regardless of whether the Applicant is accepted into the program. All non-TSA fee amounts and fee transfers between private entities will be determined and managed by the private sector and approved by all participating entities. Reimbursement fees for screeners will be billed directly to the Sponsoring Entity and will be established as a separate fee in the Federal Register to be collected by TSA via a process to be established between TSA and Sponsoring Entities.

TSA is internally coordinating RT design and operations with its other credentialing programs and programs within the U.S. Department of Homeland Security and other departments as appropriate. Where common practices are identified, TSA will pursue harmonization of processes to achieve efficiencies and strengthen customer service.

Table 2 summarizes the relationships among the various RT entities described above.

Table 2

1st Party	2nd Party(ies)	Governing Document
Enrollment Provider	Sponsoring Entity	Contract
	CIMS	MOU/Interface Control Document (ICD)
	Verification Provider	Fee transfer agreement
	TSA	Audit capability through Sponsoring Entity contract
Verification Provider	Sponsoring Entity	Contract
	CIMS	MOU/Interface Control Document (ICD)
	Enrollment Provider	Fee transfer agreement
	TSA	Audit capability through Sponsoring Entity contract
Sponsoring Entity	Service Providers (Enrollment Provider & Verification Provider)	Contract
	TSA	ASP/AOSSP; Security Directives; SOPs
CIMS	Service Providers (Enrollment Provider & Verification Provider)	MOU/Interface Control Document (ICD)
	TSA	Contract
TSA	CIMS	Contract
	Sponsoring Entity	ASP/AOSSP
	Service Providers (Enrollment Provider & Verification Provider)	Audit capability through Sponsoring Entity contract

### 1.6 Sponsoring Entity Participation

For Sponsoring Entities seeking to participate in RT, there will be a two-part process. The first part will include a statement of interest, a concept of operations, dates for implementation, and responses to questions regarding passenger volume, checkpoint configuration, and others matters to be determined by TSA. The first part may be conducted before a Sponsoring Entity has selected a Service Provider(s). The second part will include a Plan of Operations and information about the Sponsoring Entity and its agents will comply with TSA-issued RT standards.

In reviewing these submissions, TSA will work with the Sponsoring Entity to ensure that reasonable assurances exist that operations will not unduly disadvantage non-RT passengers nor decrease the quality of checkpoint security. TSA will not provide Federal funding outside the user fee structure for the launch or operations of Registered Traveler at any airport.

If a Sponsoring Entity – either on its own or on a Service Provider’s behalf – wishes to incorporate new security technology into its RT operations, TSA must first evaluate and approve it as suitable for RT operations. A Sponsoring Entity may request modifications to checkpoint security procedures based on the introduction of TSA-approved technology.

### **1.7 Relationship to Other Programs**

TSA envisions RT to be part of a greater family of biometric-based credentialing programs within DHS and the rest of the Federal Government. Under DHS leadership and consistent with the Rice-Chertoff Joint Vision, RT is coordinating with Customs and Border Protection’s (CBP) trusted traveler programs and related initiatives. These efforts are designed to identify common practices in order to realize efficiencies and enhance customer service.

TSA will continue to work through DHS, interagency working groups, and other appropriate channels to ensure that RT continues to be consistent with Federal Government efforts to integrate common practices and policies.

## **2. Eligibility**

### **2.1 Population**

Only U.S. Citizens, Nationals, and Lawful Permanent Residents (LPR) are eligible for Registered Traveler. As defined by Federal law, race, color, national origin (of citizens, nationals, and LPRs), religion, age, sex, disability, sexual orientation, status as a parent, or protected genetic information do not affect eligibility. TSA will not restrict eligibility on the basis of economic status or status in airline frequent flier programs.

### **2.2 Disposition of Minors**

The eligibility of minors who meet all other eligibility requirements will be determined based on their age. Minors under the age of 12 are not eligible to join RT but may access the RT line (and dedicated lane, if available) in the company of a parent or legal guardian that is an RT Participant in good standing. Minors above the age of 12 are eligible to join on the same basis and through the same process as adults with the additional requirement that a parent or legal guardian must be an approved RT.

### **2.3 Other**

RT Applicants agree to provide sufficient biographic and biometric data to enable: 1) TSA to conduct (and adjudicate if necessary) a Security Threat Assessment<sup>3</sup> and 2) Verification Providers to provide verification services at RT Kiosks.

RT Applicants must be able to receive and maintain an approved STA determination.

---

<sup>3</sup> Security Threat Assessments are TSA-conducted checks against Government databases to determine eligibility for RT. See Section 3.5 for more information.

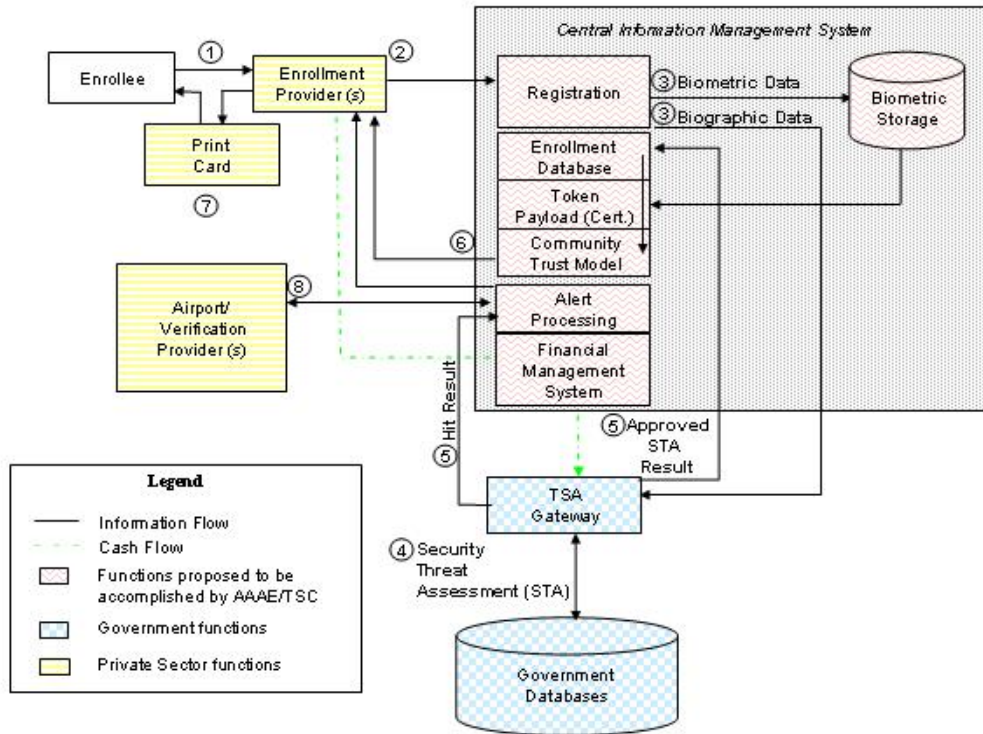
RT Applicants must agree to abide by the terms provided to them by the Enrollment Providers during the enrollment process and must remain current in the payment of user fees.

### **3. Functional Elements of the RT Program**

#### **3.1 Introduction**

Figure 1 demonstrates the flow of information among and the different responsibilities of the various RT entities. It includes the following steps: The Enrollment Provider collects biographic and biometric information from an RT Applicant and transmits to the CIMS (Steps 1 and 2). The CIMS formats and transmits the data to TSA (Step 3). TSA conducts a Security Threat Assessment at application and re-vets on a perpetual basis (Step 4) and transmits an approved or not approved finding back to the CIMS (Step 5). The CIMS informs the Enrollment Provider of acceptance or not acceptance (Step 6), and the Enrollment Provider informs the RT Applicant and issues a card if he or she is approved (Step 7). When an RT Participant travels through a participating airport, he or she uses the RT card at a RT kiosk which confirms the individual's identity and current status in the program (Step 8).

Figure 1



### 3.2 Pre-enrollment

Enrollment Providers under agreement with a Sponsoring Entity and having been authorized through the Verification and Validation process will collect and verify the biographic and biometric data of eligible RT Applicants. Biographical data may be provided by RT Applicants via the Internet if Service Providers choose to offer web-based pre-enrollment.

Pre-enrollment over the web will be an “opt-in” process via a secure website provided by the Enrollment Provider. Individuals may use this system to learn about the program and, if they decide to apply, to submit biographical information. The content of each Enrollment Provider’s site will vary and shall include privacy policies, a list of acceptable enrollment documents, and additional benefits, as well as functions to arrange appointments for enrollment and to pay user fees. Enrollment Providers may give RT Applicants the option of omitting the pre-enrollment stage and completing the entire enrollment process in person at a designated enrollment facility.

Regardless of whether an individual opts to pre-enroll, identity authentication documents and biometric data must be collected through an in-person enrollment process.

TSA is working with CBP and other Government agencies to facilitate common enrollment across different travel credentialing programs. TSA expects to phase-in the capability to give RT Applicants the option to provide additional information required for enrollment in other programs. TSA will share that information to the programs that the RT Applicant specifies. Providing or not providing this additional information is at the discretion of the RT Applicant and is not a condition for eligibility in Registered Traveler. Similarly, applicants to other programs would be able to have their other programs provide enrollment information to TSA for TSA to conduct a Security Threat Assessment for the purposes of joining RT.

### **3.3 Enrollment**

#### **3.3.1. Documents**

TSA-issued RT standards will include a list of acceptable documents used to establish identity for the purposes of the program. This list will be based on Federal form I-9, per TSA's general policy to remain consistent, where possible, with established Federal programs.<sup>4</sup> RT Applicants will be required to present documents from the TSA-established list to serve as proof of identity and, if applicable, proof of permanent residency.

Service Providers will verify the identity source documents using a front-end validation device or other state-of-the-art document authentication technologies that takes advantage of anti-fraud features incorporated into Government-issued documents.

#### **3.3.2. Biographic Data**

The Enrollment Provider will request the biographic data listed in this section. This information will be used to conduct and adjudicate the STA. If the information is not available, the Applicant should answer the field "N/A." If the Applicant does not provide all requested biographic information, it may delay or prevent an approved determination of the STA necessary to join RT. Where applicable, the Alien Registration Number for naturalized citizens – found directly below the Naturalization Certificate Number – is particularly helpful in establishing eligibility.

Providing the Social Security Number is optional; however, if the RT Applicant chooses to provide this information, it is likely to facilitate the completion of the STA.

The following biographical information will be requested at enrollment:

1. Last Name (legal name conforming to documents presented)
2. First Name (legal name conforming to documents presented)
3. Middle Name(s) (legal name conforming to documents presented)
4. Other names used (such as maiden name or alias)
5. Gender
6. Current home address (PO Box will not be accepted)

---

<sup>4</sup> The RT program narrowed the list of acceptable documents to a subset of the Federal I-9 list.

7. Current home city
8. Current home state
9. Current home Zip code
10. Previous home addresses, city, state, Zip codes in past 5 years
11. Current primary phone number (home, work, or cellular)
12. Current secondary phone number (home, work, or cellular)
13. Current e-mail address
14. Name of employer
15. Address of employer
16. Current employer city
17. Current employer state
18. Current employer Zip code
19. Date of birth
20. Place of birth
21. Nationality
22. Alien registration number (if applicable) and arrival date in U.S. (non-U.S. citizen only)
23. Height
24. Driver's license number and state of issuance
25. Social Security Number (Optional)

### **3.3.3. Biometric Data**

Enrollment Providers will collect the maximum possible of 10 flat fingerprint images. In cases where physical disability prevents an RT Applicant from providing 10 flat fingerprint images, the Enrollment Provider may enroll the RT Applicant by collecting at least four flat fingerprint images. TSA is exploring options for accommodating individuals with disabilities that prevent the collection of at least four flat fingerprint images.

The enrollee will also have the option of providing two iris images as a supplementary biometric for use in identity verification. If the Applicant is physically unable to provide both iris images, the Enrollment Provider may enroll the Applicant collecting one iris image. If an Applicant is unable to or chooses not to provide any iris image, it will not affect that individual's ability to enroll in RT.

The enrollee will select the primary biometric of preference for use in identity verification at the RT Kiosk.

The Enrollment Provider will collect a digital photograph at enrollment and display it on the outside of the RT card for identification purposes in a format consistent with TSA standards for RT. The photograph may assist the Verification Provider to ensure that an individual at an RT Kiosk is an RT Participant; it is a supplement to – and in no cases may be a substitute for – biometric identity verification using fingerprint or iris data. In addition, the photograph may facilitate the card’s use for non-security related ancillary benefits offered by a Service Provider that do not require identity verification by fingerprint or iris. At no time will the RT card be considered a valid Federal Government identification credential.

### **3.3.4. Privacy**

Enrollment Providers must establish a written privacy policy to govern the data collected in connection with the RT program and will be required to provide this policy, in writing, to each eligible RT Applicant. In addition, the Service Provider must provide each eligible RT Applicant with a copy of a Privacy Act statement supplied by TSA at the time of enrollment. TSA will use the Privacy Act as the baseline for developing RT program privacy requirements.

Pursuant to a contract with TSA, the CIMS must comply with the Privacy Act of 1974, 5 U.S.C. §552a, and the Federal Information Security Management Act (FISMA), (P.L. 107-347) to ensure the privacy and security of the data collected and submitted to TSA.

Service Providers and the CIMS may not sell or disseminate any biographic and/or biometric data collected by Service Providers from RT Applicants for any commercial purposes without the explicit approval of the RT Applicant. Service Providers can only collect information for non-RT purposes through an “opt-in” process on a separate form from the RT data. No RT Applicant will be denied on the basis of not providing any “opt-in” information to the Service Provider.

Before implementation, TSA will publish a Privacy Impact Assessment (PIA) for Registered Traveler concerning the storage and use of personal information. The Enrollment Provider will only store the necessary information required for customer service and card re-issuance. The Verification Providers will not store RT Participants’ personal data except as specified in TSA standards for RT. For each RT Participant, the CIMS will only store an anonymous RT identification number, biometric information (needed to check for duplicate applications), renewal date, an approved or not approved STA finding, and other information as directed by TSA. The CIMS is not expected to store biographic information.

All Enrollment Provider personnel who handle RT Applicants’ and Participants’ personal information must be properly trained and vetted in accordance with all TSA-issued RT standards to perform necessary enrollment procedures and use required technology. Access to enrollment workstations will require biometric authentication by an authorized Enrollment Provider technician at each individual enrollment. TSA standards for RT will include checks and balances (such as signatures from multiple individuals at collection and submission of enrollment data) to ensure security cannot be compromised by one individual within the system.

### **3.4 Central Information Management System**

#### **3.4.1. Transmittal**

Enrollment Providers must securely transmit application enrollment data to the CIMS. Service Providers should submit only the data necessary for TSA to complete the STA. Any additional information collected by Enrollment Providers should not be transmitted to the CIMS. The CIMS will format all data from the Enrollment Providers and pass it through to TSA in a manner prescribed by TSA.

The CIMS will receive and format enrollment data from Enrollment Providers and transmit the necessary data to TSA or other Federal entities as defined in the forthcoming PIA for RT. The CIMS will also validate and perform duplicate checking of received biometric enrollment data with biometric data currently stored in the CIMS database.

#### **3.4.2. Duplicate Check**

To identify potential security threats, the CIMS will identify cases where a new enrollment has the same biometric but different biographic information as an existing enrollment and notifying TSA for resolution. CIMS will conduct a duplicate check on all Applicants to determine if an RT record already exists for the submitted biometrics. This check will consist of a One-to-Many (1:n) match of the RT Applicants' submitted biometric against its database of RT Participants' biometric image data. This database contains the biometric data, an anonymous RT identification number, and current status for all RT Participants. As a privacy safeguard, it does not contain RT Applicants' biographic information. When a potential match occurs, the CIMS will receive temporary access to the relevant biographic data in order to determine whether the biographic data for the potential duplicates is the same.

As necessary, TSA will conduct further adjudication and determine a course of action. If the biographic information is consistent, a link will be created between the relevant unique identifiers and the application will proceed normally. If the biographic information is not consistent, TSA will take appropriate measures, including possible referral to law enforcement or intelligence agencies.

### **3.5 Security Threat Assessment**

TSA will be responsible for conducting and adjudicating the STA for all RT Applicants before acceptance and for all RT Participants on an ongoing basis. The STA's scope and components are subject to change and will largely correlate to the types of benefits offered at the security checkpoint and the overall security environment.

The STA includes running the volunteers' information through terrorist-related databases, criminal databases for outstanding warrants, and other government databases that TSA maintains or uses in order to confirm that volunteers are U.S. citizens, lawful permanent resident aliens or nationals of the United States, and to ensure that the volunteer does not pose or is not suspected of posing a threat to transportation security.

If the check indicates a potential match, TSA will adjudicate the result to ensure its validity and, where appropriate, may contact the individual for additional information. After adjudication, the names of persons considered to be posing or suspected of posing a threat to aviation security will be forwarded to appropriate law enforcement and/or intelligence agency(ies) for either action or further investigation.

TSA will communicate the results of the STAs to the CIMS when a determination is reached. TSA will not transmit details about the STA or the reasons behind its determination.

The CIMS will inform the submitting Enrollment Providers about the RT Applicants' STA results. The Enrollment Provider is responsible for informing the RT Applicant of the result – usually in conjunction with issuing the RT card if the RT Applicant is accepted.

For RT Applicants with an approved STA result, the CIMS will generate a digital payload for storage on the RT card. The digital payload will include a unique RT identification number, biometric templates for identity verification, a pointer that prompts the RT Participant to the biometric which he (she) selected for verification purposes, and other data relevant to the RT verification process. The process will ensure a complete chain of trust from vetted enrollments to the issued credential and facilitates interoperability.

Applicants who do not receive an approved STA result (and consequently cannot participate in RT) will be able to seek redress through TSA's Office of Transportation Security Redress.

### **3.6 Card Production and Issuance**

The Enrollment Provider will be required to produce cards for its RT Participants' that meet TSA standards for security that implements reasonable safeguards (as defined in TSA standards) to ensure no unauthorized production occurs. As will be established in TSA standards, cards will conform to current Federal Technical Implementation Guidance and biometrics will be stored consistent with biometric standards established by the American National Standards Institute/InterNational Committee for Information Technology Standards (ANSI/INCITS). Security requirements should meet appropriate FIPS requirements as defined in the TSA-issued RT standards. Using language to be set forth in the TSA standards for RT, the Enrollment Provider will mark the RT cards to indicate clearly that they are not valid Government identification credentials and that penalties may be levied for fraudulent or unauthorized use.

On the outside of the card, a required uniform RT logo will serve as an accreditation logo and will be visible on the card. A digital photograph of the RT Applicant will also be placed on the outside of the cards in a manner consistent with TSA standards designed to minimize the chance that the card could be confused with a Federal identity credential for non-RT purposes. The Service Provider's and/or Sponsoring Entity's logo(s) can also be featured on the card to facilitate non-security related benefits. Individual Service Providers will determine (subject to TSA approval) what else may or may not appear on the outside of the card.

The Service Providers will be responsible for the quality of the RT cards used as well as the replacement of any lost, stolen, damaged or destroyed RT cards. The Service Provider may offset costs associated with these responsibilities through the private sector-portion of the user fees.

### **3.7 Program Fees and Membership Renewal**

The total RT participant fee will consist of two parts: the TSA-set portion and the private sector portion. The private sector portion of the fee will be set and collected by the Enrollment Providers. Although the TSA portion of the fee will be consistent among all RT Participants, the private sector portion of the fee may differ between Enrollment Providers depending upon individual costs and benefits of applicable services.

TSA anticipates that the private sector fees will include compensation to the CIMS, as well as any costs of providing ancillary services and/or dedicated lanes and screening equipment. TSA will not compensate the Verification Provider or Sponsoring Entity nor determine the method by which they will be compensated.

TSA's activities under RT will be completely funded through the fees set by TSA through notice in the Federal Register. While still under development, the TSA portion is expected to be up to \$30 per RT Applicant (or Participant) per year. This fee may include components determined on a per RT Applicant (or Participant) basis and/or amounts related to TSA's costs in fulfilling its responsibilities related to RT oversight and operations. The fee range given is an estimate and may deviate significantly from this estimate at the point of publication in the Federal Register. The reason for such adjustments, as well as for adjustments required in the future, may be due to changes in key input (e.g., the estimated vs. actual quantity of RT participants) or various cost components (e.g., costs associated with an expanded STA or new technologies).

Cost associated with TSOs will not be paid through the TSA portion of the user fee (i.e., the up to \$30 per RT Applicant/ Participant per year fee cited above). Sponsoring Entities will reimburse TSA for the RT use of TSOs at a rate that will likely range from \$140 to \$300 per hour (i.e., \$35-\$50 per TSO per hour for four to six TSOs per lane). This range should be considered a guideline for planning purposes. The actual rate may vary at individual airports due to local conditions.

The CIMS will be responsible for monitoring the enrollment dates of all participants and deactivating their RT membership in the absence of renewal. Enrollment Providers will collect renewal fees for their members. The FMS will serve as the point of interface among TSA, Sponsoring Entities, and Service Providers for the TSA portion of initial and annual fees. At program launch, the CIMS and FMS will be a single entity.

TSA will require an annual fee for each Participant – on a rolling basis based on the date of acceptance into RT – collected by Enrollment Providers and paid to TSA through the FMS, as well as any separate reimbursement fees for TSOs charged to the Sponsoring Entity. Since all pertinent information on RT Participants is stored at TSA for perpetual vetting, a resubmission of this data will not be required. Biometric data will need to be resubmitted by the RT Participants through the Enrollment Provider periodically in accordance with standards set by TSA.

TSA fees will not be refunded for initial enrollments or renewals by RT Participants.

### 3.8 Verification and Use

Unless a remote location is approved by TSA, processing of RT Participants will occur at enabled airport security checkpoints by the Verification Provider. Biometric technology using fingerprints and iris will be used for participant identity verification at the RT Kiosks. Manual verification by the Verification Provider will not be allowed in any circumstance. Proposed biometric systems will be highly accurate, cost effective, and capable of confirming the identities of large populations within short time constraints.

RT Participants will use the designated and/or dedicated RT security lines/lanes. Travelers who are not enrolled in RT or are not approved when presented at the RT processing area will be directed by the Verification Provider to use the normal TSA security lines/lanes. At the discretion of TSA and Sponsoring Entity, RT Participants who cannot be biometrically verified due to a technical error may have direct access to a non-RT lane (or selectee lane dependent on selectee status) where feasible. This procedure may prevent RT Participants who cannot use RT services due to technical reasons from being unnecessarily disadvantaged (including possibly missing flights) due to an expectation of the shorter processing time at an RT lane.

An RT Participant will present his or her RT card at the RT Kiosk. The RT Kiosk must be capable of reading the information contained on the RT cards issued by valid Enrollment Providers. The RT Kiosk will authenticate the card by: a) recognition of the issuing party, b) the integrity of the biometric templates, and c) confirmation that the information contained within it has not been tampered with. The system will then check the credential presented against the CIMS-managed participant and revocation lists to ensure that the holder is still an active and approved RT Participant.

RT Participants will select a preferred verification biometric, fingerprint or iris, during the enrollment process. Prompted by a message on the screen on the RT Kiosk, the RT Participant now presents the preferred biometric using capture devices in the RT Kiosk. RT Kiosk compares the captured biometrics to biometric templates read from the card. Three attempts at the primary biometric will be permitted. If a match exists, the RT Kiosk indicates success, the Verification Provider marks the RT Participant's boarding pass in a manner defined by the TSA-issued standards, and the RT Participant proceeds to the RT TSA security lane. If a match to the primary biometric is not made and the RT Participant chose to provide the iris biometric at enrollment, three attempts to match to a secondary biometric stored on the card will be permitted. If a match to the secondary biometric exists, the RT Kiosk indicates success, the Verification Provider marks the RT Participant's boarding pass in a manner defined by the TSA-issued standards, and the RT Participant proceeds to the RT TSA security lane. Otherwise, the RT Participant is directed to the general passenger TSA line by the Verification Provider using the procedures outlined above.

A biometric match at the RT Kiosk would verify the RT Participant's biometrics captured at that moment against the biometric templates stored on the card. Biometric capture should take less than two seconds per each attempt, allowing timely throughput. This does not include the time needed for the RT Participant to position his or her finger or eyes for the capture device.

Verification Providers will operate the RT Kiosks, including the timely update of system and card revocation status to ensure fast, secure and reliable verification and status-checking at the airport checkpoint. The information at the RT Kiosk must be protected against compromise through encryption technologies and physical security configuration established in the TSA-issued RT standards.

### **3.9 Credential Revocation List**

TSA or the Participant's Enrollment Provider can revoke a RT Participant's membership in RT. TSA can revoke any and all cards for security reasons – such as if a RT Participant no longer has an acceptable STA. Enrollment Providers will be responsible to determine the need for any other revocations, such as those for non-payment, as well as for informing the CIMS of any lost, stolen or damaged cards. The Enrollment Provider that issued the RT card is the only Service Provider able to determine the need to revoke that card. The entity revoking a RT Participant's membership will provide the CIMS with the unique and anonymous identifier tied to the Registered Traveler's enrollment record to the CIMS.

The CIMS will be responsible for consolidating all revocation events into a single credential revocation list and ensuring its distribution to RT Verification Providers (either by sending the list to the VP or by a system where the VP reliably requests it) in a manner consistent with TSA standards.

Upon notification of revocation, the CIMS will immediately communicate revocations to all Verification Providers and the RT Participant's Enrollment Provider by RT number. Verification Providers will update their RT Kiosks as soon as possible and within a time period to be determined in TSA-issued RT standards, depending on their level of connectivity.

### **3.10 Standards and Conformance**

All RT Service Providers must be sponsored by a Sponsoring Entity (i.e., airports and/or air carriers) and must meet TSA-issued RT standards.

Service Providers must stay in compliance with TSA-issued standards. These standards will be incorporated into the appropriate regulatory security documents of the Sponsoring Entity to enable their enforcement. The standards will also be the basis of the CIMS and be included in agreements establishing the CIMS.

It is the responsibility of a Sponsoring Entity to ensure that its chosen RT Service Provider(s) meets TSA-issued RT standards. TSA expects that its standards will require each Service Provider to obtain an independent auditor, in accordance with guidelines determined by TSA, to ensure compliance with TSA standards. The Service Provider will fund the independent auditor, and the Sponsoring Entity will send a copy of all reports to TSA. Service Providers will be subject to Validation and Verification oversight by their Sponsoring Entity and by TSA.

TSA will also require interoperability testing through the CIMS prior to operations. Interoperability testing will focus on the technology and accompanying hardware.

## **4. Security Procedures and Benefits**

### **4.1 RT Screening Procedures and Security Related Benefits**

TSA expects that benefits will be linked to the ability of the private sector to identify and invest in innovations. Sponsoring Entities and Service Providers may recommend new technologies and practices that may provide an equivalent or higher level of security to current procedures. TSA will evaluate such proposals based on three criteria: 1) their ability to maintain or enhance security; 2) their prospects for implementation at no cost to TSA; and 3) their impact on non-RT wait times. If TSA determines that a proposal meets these criteria, it may institute changes in checkpoint requirements at locations where this innovation is introduced.

Security benefits offered through Registered Traveler are at the sole discretion of TSA and are subject to change at any time. Security benefits will be based on the current security posture, the scope of the STA conducted on RT Participants, and the integration of available technology and operating procedures at specific RT checkpoints. An element of unpredictability will be used throughout the program so that a RT Participant's experiences may vary to a limited extent when he or she travels. In addition, all RT Participants are subject to additional screening at the discretion of the TSOs.

The following processes may be implemented at the RT checkpoint line and lane in addition to the STA:

1. RT Participant will present a smart card at an RT Kiosk to link an approved STA with his or her identity.
2. All RT Participants will be required to be screened by the Walk Through Metal Detector (WTMD) and have all carry-on luggage pass through the x-ray equipment. All RTs will be required to go through additional screening to resolve any alarms during the screening process.
3. Integration of additional technologies that can facilitate throughput and convenience to passengers as it becomes available and passes certification.
4. Allowing dedicated lines with either integrated or dedicated lanes.
5. Institute changes to operations designed to accelerate the screening process of RT Participants without diminishing security.

TSA will continue to work with Sponsoring Entities and industry stakeholders to explore any additional benefits that may be made available based on changing technologies and conditions. As a result, benefits and security measures will continue to evolve.

### **4.2 Ancillary (non-security) Benefits**

Additional program benefits not pertaining to security are not determined or managed by TSA. These benefits may enhance customer service and be part of the competitive framework of the

overall program. These benefits may include, but are not limited to, discounts on services or concessions and technology and/or equipment at the checkpoints to facilitate convenience to the passenger. These benefits are solely at the discretion of the private sector. Any additional personal information required for these benefits must be provided on “opt-in” forms separate from the data collected under TSA direction for the STA.

## **5. Data Transfer and Storage Model**

All Service Providers, TSA, the CIMS, the Sponsoring Entities, and any other Federal Government or private sector participant that will touch RT data will be required to provide a fully integrated layered security structure outlined in the standards issued by TSA. All relevant data will be encrypted at the initial collection point and remain encrypted -throughout the process. All data transfers of information will require authentication handshakes at both ends and all data used in the verification process will require digital signatures to facilitate chain of custody throughout the system. All Service Providers will be in compliance with TSA standards that will be based on appropriate sections of Federal Information Security Management Act (FISMA). The CIMS and the Federal Government-run systems will meet all FISMA requirements.

All Service Providers and Sponsoring Entities must meet the qualification and verification and validation requirements outlined in this model to continually provide RT services.

## Appendix A: Common Terms and Definitions

Following are common definitions of key terms used throughout the model:

- **Aircraft Operator Standard Security Program (AOSSP):** A standardized program for domestic aircraft operators for flights both in the United States and Overseas that are regulated in accordance with 49 CFR Part 1544. It contains requirements for areas such as training area and aircraft security. Screening is included.
- **Airport Security Program (ASP):** The term ASP refers to the local program for that specific airport. National Amendments to ASP's are issued from headquarters requiring amendments to all local programs. There is no standardized program for airport operators regulated in accordance with 49 CFR 1542.
- **Dedicated Lane:** TSA screening operation used exclusively for Registered Traveler Participants.
- **Dedicated Line:** A queue to the TSA checkpoint lane used exclusively for Registered Traveler Participants.
- **Financial Management System (FMS):** A system to collect and distribute the TSA user fees to TSA from Sponsoring Entities/Service Providers.
- **Integrated Lane:** TSA screening operation used primarily (but not exclusively) for Registered Traveler Participants.
- **Integrated Line:** A queue to the TSA checkpoint lane used primarily (but not exclusively) for Registered Traveler Participants.
- **Interoperability:** The technical capability for any RT credential legitimately issued by an RT Enrollment Provider to work at the Kiosk of any authorized Verification Provider.
- **Lawful Permanent Resident (LPR):** An individual who has been lawfully admitted to the United States for permanent residence, as defined in 8 U.S.C. §1101.
- **National of the United States:** As defined in 8 U.S.C. §1101, a citizen of the United States or a person who, though not a citizen of the United States, owes permanent allegiance to the United States.
- **Privacy Act:** The Privacy Act of 1974, 5 U.S.C. §552a, which governs the collection, maintenance, use, and dissemination of information contained in a system of records as defined by the Act.
- **Security Threat Assessment (STA):** The process by which TSA determines an RT Applicant's initial eligibility for the program, as well as RT Participant's continued eligibility. The STA includes checks against Federal Government databases and adjudication.
- **TSA Screening Gateway:** TSA-run information technology system used to facilitate the Security Threat Assessments and interface with the Central Information Management System.

- **Validation and Verification:** Process for establishing that Service Providers meet the TSA-set standards needed for authorization to provide enrollment and/or verification services.