Privacy Impact Assessment
for the

Registered Traveler Interoperability Pilot

September 1, 2006

Contact Point
John Martinez
Director, Registered Traveler Program
Transportation Security Administration
Registered.Traveler@dhs.gov

Reviewing Officials
Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration
TSAPrivacy@dhs.gov

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
571-227-3813

Abstract

The Aviation and Transportation Security Act (ATSA), P.L. 107-71, Section 109 (a)(3), authorizes the Transportation Security Administration (TSA) to "establish requirements to implement trusted passenger programs and use available technologies to expedite security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening." Pursuant to that authority and following two sets of pilot programs, TSA is conducting the next phase of Registered Traveler (RT) at approximately 10-20 participating airports to further test and evaluate this type of trusted passenger program. This phase, known as the Registered Traveler Interoperability Pilots (RTIP), follows the results of two sets of previous RT pilots conducted by TSA in 2004-05. This phase introduces interoperability among participating airports/air carriers and operating with larger populations.

Introduction

Under Registered Traveler, travelers who are U.S. citizens, lawful permanent resident aliens or nationals of the United States, volunteer to undergo a TSA-conducted security threat assessment in order to confirm that they do not pose or are not suspected of posing a threat to transportation or national security.

RT is a private sector program, supported and overseen by TSA, with distinct roles and responsibilities for each participating entity. TSA is responsible for setting program standards, conducting the security threat assessment, physical screening at TSA checkpoints, and certain forms of oversight. The private sector is responsible for enrollment, verification, and related services.

To enroll, applicants voluntarily provide RT Sponsoring Entities (i.e., participating airport authorities or air carrier operators) and Service Providers (i.e., a private sector vendor chosen by a Sponsoring Entity to implement RT as its agent) with biographic and biometric data needed for TSA to conduct the security threat assessment and determine eligibility. The security threat assessment includes checking each applicant's identity against terrorist-related, law enforcement, and immigration databases that TSA maintains or uses. RT applicants who receive an "approved" security threat assessment result may become program participants.

Once a traveler qualifies as an approved participant, the traveler would be able to take advantage of the expedited screening process available exclusively through the Registered Traveler program. During the RT process, participants verify their identity through biometric identity verification technologies at the screening checkpoint. This process also ensures that the individual is a currently "approved" RT participant. After the identity and current status of the RT participant are verified, the participant enters the checkpoint lane identified for registered travelers and undergoes the applicable TSA checkpoint screening. This process should provide the basis to expedite the screening of RT participants.

Because this program requires the collection of personal information about members of the public, TSA is required under Section 208 of the E-Government Act of 2002, P.L. 107-347, and the accompanying guidelines issued by the Office of Management and Budget (OMB) on September 26, 2003 and Section 222 of the Homeland Security Act of 2002, P.L. 107-296, and the accompanying guidance issues by the DHS Privacy Office, to issue a Privacy Impact Assessment (PIA). The PIA is based on the current design of the program and the Privacy Act system of records notices, DHS/TSA 002, Transportation

Security Threat Assessment System, which was last published in the Federal Register on November 8, 2005, 70 FR 67731-67735, and DHS/TSA 015, Registered Traveler Operations Files that was last published in the Federal Register on November 8, 2005, 70 FR 67731, 67735.

Background

Before this Registered Traveler Interoperability Pilot (RTIP), there were two previous sets of pilots designed to test different aspects of Registered Traveler. The first phase of RT development was the federally-managed pilot at five designated airports that established the basis of the program (biometrics used in identity verification) and developed the initial parameters (determine baselines for public acceptance and success of biometric usage). The second tested the feasibility of implementing RT through a public / private partnership at a single airport.

RTIP is expected to include approximately 10-20 airports. These airports will begin participating in RTIP as Sponsoring Entities once they make the necessary business arrangements with Service Providers and obtain TSA approval for the proposed configuration for RT operations at that airport. This implementation approach allows TSA to confirm the private sector's ability to provide interoperability among RT airports, evaluate possible means to expedite screening for participants, and re-affirm that RT continues to maintain TSA's high security standards. As authorized by TSA, the RTIP is intended to strengthen customer service for eligible air travelers while maintaining security at the TSA screening checkpoint.

Under RTIP, Sponsoring Entities contract with Service Providers to perform enrollment and verification services. An RT Service Provider can be: 1) an Enrollment Provider (EP) that collects the biographic and biometric information from RT Applicants, collects user fees from RT Applicants, and issues RT cards to RT participants; 2) a Verification Provider (VP) that confirms that the RT Participant is an active participant in accordance with TSA-issued RT standards; or 3) a combined Enrollment and Verification Provider. "Service Provider" is used in this document as a term of collective reference to RT vendors of all three categories.

Private sector Service Providers must meet qualification and participation criteria set by TSA in order to participate, including security requirements and oversight. Oversight may include (but is not limited to) announced and unannounced inspections of the Service Provider by TSA or by the Sponsoring Entity, the collection of metrics, and reconciliation of records among TSA, and reviews of the Service Providers' information technology security systems and documentation. The Sponsoring Entity is responsible for ensuring that these Service Providers meet TSA-mandated standards. TSA enforces these standards through the Sponsoring Entity (airport or air carrier), which is subject to inspection and regulation by TSA.

During RTIP, the Enrollment Provider will accept applications from individuals who wish to participate. Enrollment is voluntary and is not a precondition for flying commercially. Eligible candidates must be US citizens, US nationals, or lawful permanent residents of the United States and meet any other eligibility requirements set by TSA and the Enrollment Provider (See Appendix A for eligibility requirements). Enrollment Providers, acting as agents of their respective Sponsoring Entities, will enroll eligible applicants by collecting biographic and biometric information, examining Government-issued identity documents, and transmitting necessary information to TSA and through a TSA-designated Central Information Management System (CIMS).

Central Information Management System

TSA will enter into a contract with a private sector entity to create and operate the Central Information Management System (CIMS). The CIMS aggregates, stores and distributes information (on an as needed basis) to the Service Providers participating in RT. The contractor's responsibilities include: receiving, aggregating, and formatting RT applicant data from Enrollment Providers; performing checks to identify potential duplicate biometric enrollments through the retention of fingerprint and iris templates to ensure application integrity; transmitting applicant biographic data to TSA for the agency to conduct Security Threat Assessments; receiving the determination of eligibility from TSA; maintaining and distributing the Credential Revocation list (consisting of a unique number) issued to each RT applicant and participant); and generating the biometric payload and encryption protocols for RT cards. The CIMS contractor will be contractually obligated to comply with the Privacy Act of 1974, 5 U.S.C. §552a, and the Federal Information Security Management Act (FISMA), (P.L. 107-347) and DHS Privacy Office privacy policies to ensure the privacy and security of the data received, transmitted to and retained by TSA and the CIMS.

As part of the partnership arrangement, TSA will conduct security threat assessments and fingerprint-based criminal history records checks on the Service Providers' key personnel. TSA seeks to ensure that the persons conducting enrollment and verification operations or responsible for managing such persons do not pose or are not suspected of posing a threat to transportation or national security.

TSA will identify cases where a new enrollment has the same biometric but different biographic information as an existing enrollment. When a potential duplicate occurs, TSA will conduct further adjudication and determine a course of action on duplicate biometric applications with inconsistent biographic data. If the biographic information is consistent, a link will be created between the relevant unique identification number and the application process will proceed. If the biographic information is not consistent, TSA will take appropriate measures, including possible referral to law enforcement or intelligence agencies.

Security Threat Assessments

Using the information provided, TSA conducts a security threat assessment to ensure that the applicant is not suspected of posing a threat to transportation or national security. Once the applicant is successfully enrolled the participant will be perpetually vetted. The security threat assessment includes checking the applicants' information against terrorist-related, law enforcement, and immigration databases that TSA maintains or uses in order to confirm that applicants are U.S. citizens, lawful permanent resident aliens or nationals of the United States, and to ensure that the applicant does not pose or is not suspected of posing a threat to transportation or national security. TSA will communicate directly with the applicant to request additional information if necessary to adjudicate an application and may also notify the Enrollment Provider of the status of the security threat assessment for that individual.

TSA transmits approval status back to the RT Enrollment Provider acting as an agent of their Sponsoring Entity but does not transmit any other information generated during the security threat assessment. "Approved" applicants will receive confirmation of acceptance and an RT card from the Enrollment Provider that will allow them to use RT screening checkpoint lines/lanes at all participating airports. If the security threat assessment results in a "not approved" status, TSA will inform the individual

directly, as well as notify the CIMS, which, in turn, will notify the Sponsoring Entity/Enrollment Provider. If an RT applicant does not meet the Enrollment Provider's standards, such as non-payment of enrollment fees, and is "not approved," the Enrollment Provider will inform the applicant directly, as well as notify TSA via the CIMS. Applicants who receive a "not approved" security threat assessment result will be given the opportunity to contact TSA to address their concerns.

Access to Information

The Enrollment Provider will be required to produce and issue cards to its approved RT participants. This card must meet TSA security standards, including use of reasonable safeguards (as defined in TSA standards) to ensure security and that no unauthorized card production or copying occurs. Additionally cards will contain an RT applet which will govern interaction between the card reader and the RT information on the card.

Prior to entering TSA RT screening checkpoint lanes, the participant must present his or her RT card and verify their biometric (fingerprint and/or iris) at the Verification Provider's kiosk to confirm his or her identity as a current, "approved" RT participant. Information stored in the RT applet is limited. The card contains only enough biometric data to confirm a person's identity when he or she travels. Biometric data will be associated with a unique identifier to confirm that the traveler is an active RT participant. As a safeguard against biometric theft, fingerprints are not stored on the RT card as an image, but rather as a template which prevents unauthorized parties from replicating the full biometric image. Some private entities may add items to the RT card for such purposes as marketing, billing, or tracking usage.

Table 1 details which entities will have access to personal information during the course of an individual's RT membership. "Retained," as used in Table 1, is defined as storing and maintaining the specified data in the normal course of duty following an individual's acceptance in Registered Traveler. During the enrollment process, TSA may receive and temporarily store biometric data and CIMS may receive and temporarily store biographic data. Furthermore, after a person has been accepted into RT, the CIMS and/or TSA may receive and temporarily store data that it does not normally store in order to accomplish a specific security function, such as adjudication.

Table 1

	Private Sector Systems Boundary		**Government Systems Boundary**	
	RT Card (individual)	**Service Provider** (its members only)	**CIMS** (all members)	**TSA** (all members)
Unique Identifier	Retained	Retained	Retained	Retained
Biographic Information	Name will be printed on the card but Not Stored or Retained on the program applet	Retained	Temporary Access and Storage may occur; Not Retained	Retained
Biometric Images	Accessed,	Retained	Retained	Access, Storage,

	Stored and Retained only if iris provided			and Retention will occur for adjudication or national security purposes
Biometric Templates	Accessed, Stored and Retained for fingerprints	Retained	Accessed, Stored and Retained	Temporary Access and Storage may occur; Not Retained
Copy of Identity Documents	Not Accessed, Stored or Retained	Retained	Not Accessed, Stored or Retained	Access, Storage, and Retention may occur for adjudication or national security purposes
Security Threat Assessment Determination	Not Accessed, Stored or Retained	Retained	Retained	Retained
Security Threat Assessment Case History	Not Accessed, Stored or Retained	Not Accessed, Stored or Retained	Not Accessed, Stored or Retained	Retained
Billing Information	Not Accessed, Stored or Retained	Retained	Not Accessed, Stored or Retained	Not Accessed, Stored or Retained

Note 1: The RT card will be solely in the possession of the individual. The Service Provider will store only information concerning the individuals that it enrolled. The CIMS and TSA will store data on all RT members.

Note 2: The security threat assessment case history includes the information that TSA receives from the terrorist-related, law enforcement, or immigration databases used for the security threat assessment process.

Note 3: TSA will retain information in accordance with its records retention schedule approved by the National Archives and Records Administration (NARA). The CIMS will retain information in accordance with the contract with TSA, which will ensure retention in accordance with a records retention schedule approved by NARA. Service Providers will retain information in accordance with their respective privacy policies.

Note 4: Iris images may be shared with the National Institute of Standards and Technology (NIST) for purposes of research to develop government standards for the use of iris images. Iris images will be shared with NIST only after TSA enters into a Memorandum of Understanding to minimize privacy impacts and secure the data. Participation is strictly voluntary and individuals will separately opt-in to share images with NIST for future research purposes.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

Registered Traveler (RT) Applicant - Biographic Data

The following biographic information will be requested from RT applicants at enrollment in order for TSA to conduct and adjudicate a name-based security threat assessment:

- Full legal name (as listed on the Government-issued identity documents used to establish identity),
- Other names used,
- Social Security number (optional),
- Citizenship status,
- Alien registration number (if applicable),
- Current home address,
- Primary and secondary telephone numbers (home, work, or cellular),
- Current email address,
- Date of birth,
- Place of birth,
- Gender, and
- Height.

Provision of the requested information, including Social Security number, is voluntary. However, if the applicant does not provide all of the requested biographic information, it may delay or prevent an "approved" determination of the security threat assessment necessary to join RT.

The following data is optional but may facilitate adjudication without requiring the individual to provide the information and process set forth in section 7.2:

- Prior home addresses (for the past five years),
- Driver's license number, and
- Employer name and address.

This information would be used to assist in distinguishing the individual from a possible match to an individual in Federal watchlists when other enrollment data is insufficient to distinguish the individual.

RT Applicant - Biometric Data

In order to issue an RT card, TSA requires that the Enrollment Providers collect fingerprint images at enrollment in order to perform a biometric-based identity verification procedure prior to the RT participant entering the TSA security checkpoint to ensure that the individual is a currently "approved" RT participant.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 further accommodating persons with disabilities that prevent the collection of at least four flat fingerprint images.

TSA also requires EPs to have the capability to collect iris images. The applicant will have the option of providing two iris images as a supplementary biometric for use in verifying his/her enrollment status

prior to entering the TSA security checkpoint at the airport. If the Applicant is physically unable to provide both iris images, the Enrollment Provider may enroll the Applicant collecting one iris image.

It is possible that iris images may also be used in research solely to develop NIST standards of the use of iris data only when expressly volunteered by the individual for this purpose.

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.

Service Provider Personnel

Before a Service Provider may begin offering RT services, it must demonstrate that it meets TSA-issued RT standards. As part of these standards, the Service Provider's key personnel (defined in section 1.2) must submit biographic information and 10-fingerprint images for a fingerprint-based criminal history records check and a name-based security threat assessment:

Full legal name (as listed on the Government-issued identity documents used to establish identity),

- Other names used,
- Citizenship status,
- Alien registration number (if applicable),
- Current home address,
- Primary and secondary telephone numbers (home, work, or cellular),
- Current email address,
- Date of birth,
- Place of birth,
- Gender, and
- Height.

If the employee does not provide all requested biographic information, it may delay or prevent the completion of the security threat assessment. The following data fields are optional but may facilitate any necessary adjudication of the security threat assessment:

- Prior home addresses (for the past five years) and
- Driver's license number.

This information will be used to assist in distinguishing the individual from a possible match to an individual in Federal watch lists when other enrollment data is insufficient to distinguish the individual.

The following additional biographic information will be requested from Service Provider personnel in order for TSA to conduct a fingerprint-based criminal history records check in accordance with Federal form FD-258: Social Security number, armed forces number (if applicable), employer name and address, race, weight, eye color, and hair color.

1.2 From whom is information collected?

RT Applicant/Participant

RT applicants' biographic information is collected directly from the applicant by the private sector Enrollment Provider that must be sponsored by a Sponsoring Entity (i.e., participating airport authority or air carrier operator). TSA will receive the applicants' biographic information from the Enrollment Provider via the CIMS.

RT applicants will also be asked to provide biometric data at the time of enrollment. Prior to entering a TSA security screening checkpoint lane, an RT participant must present a biometric (fingerprint or iris image) at a kiosk operated by the Verification Provider. This biometric is matched against the biometric template stored on the RT card to confirm identity and verify the person's status as a current, "approved" RT participant.

Service Provider Personnel

TSA-issued RT standards require that all key personnel of Service Providers and their subcontractors provide personal information to TSA necessary to conduct a fingerprint-based criminal history records check and a name-based security threat assessment. Key personnel are defined as: 1) officers, principals, and program managers responsible for RT operations; and 2) all employees that collect, handle or use RT applicant or participant data.

1.3 Why is the information being collected?

RT Applicant/Participant

Biographic information is collected from RT applicants to conduct an initial security threat assessment on applicants and a perpetual security threat assessment on participants throughout their membership in the program. TSA will compare the applicants' information against terrorist-related, law enforcement, and immigration databases that TSA maintains or uses in order to confirm that applicants are U.S. citizens, lawful permanent resident aliens or nationals of the United States, and to ensure that the applicant does not pose or is not suspected of posing a threat to transportation or national security. Email address and telephone numbers are collected to facilitate administrative communication with the applicant / participant. The biometric information will be used to issue each "approved" participant an RT card linked to his or her biometric information and enable the verification provider to verify the individual's status as a currently "approved" RT participant before allowing the individual to proceed to the TSA security checkpoint at the airport.

Service Provider Personnel

Information collected on Service Providers' and their subcontractors' key personnel (as defined in section 1.2) will be used to conduct fingerprint-based criminal history records checks and name-based security threat assessments to ensure that the employees responsible for RT operations do not pose or are not suspected of posing a threat to transportation or national security.

1.4 What specific legal authorities/arrangements/ agreements define the collection of information?

Under 49 U.S.C. § 109(a)(3), TSA may establish the registered traveler program. Under 49 U.S.C. § 114(f) TSA has broad authority to issue regulations to carry out its statutory functions.

1.5 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

The information collected will be used to verify an RT applicant's identity and to conduct a security threat assessment which will assist in determining whether the individual poses or is suspected of posing a threat to transportation or national security. This information will also be used to enable Service Providers to issue an RT card for eligible applicants. The information collected will assist TSA in eliminating confusion over an individual's identity in cases where the security threat assessment indicates a potential match to a watch list or other Federal database TSA maintains or uses for security threat assessments. The information increases the chances that adjudication can resolve the potential match without having to contact the individual and reduce the number of individuals who will provide more extensive identifying information under the processes set forth in 7.2 for redress. On balance, the few items of additional information serve privacy interests by reducing the amount of additional information that would otherwise need to be collected by TSA.

An important facet of the RT program is that participation will be strictly voluntary. If individuals are concerned about the privacy implications of providing the personal data requested for this program, they are not required to participate in the program in order to fly on a commercial air carrier.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

TSA will use information gathered from applicants for participation in RT for the following purposes:

1. To conduct security threat assessments on individuals participating in the program;
2. To use biometric verification technologies to expedite security screening at TSA security checkpoints for current RT participants;
3. To assist in the management of RT applicant records and security threat assessments;
4. To permit access on a need to know basis only to the security threat assessment status ("approved" or "not approved") of an RT participant prior to allowing them to enter a RT security screening lane at the airport;
5. To allow TSA, or the CIMS acting as TSA's agent, to identify cases where a new applicant has the same biometric but different biographic information as another RT applicant, thereby indicating a potential attempt to circumvent the enrollment process;

6. To refer to the appropriate intelligence and law enforcement entities the identity of RT applicants who pose or are suspected of posing a threat to transportation or national security; and
7. Possibly to be used by NIST in research solely to develop government technology standards for the use of iris images.

Use of information shared by the applicant to the Service Provider, beyond the specific information requested by the government for the security threat assessment will be governed by the agreement between the service provider and the individual and may include usage for other private industry services. These other uses are outside the scope of this Privacy Impact Assessment. Individuals interested in more information about other uses of other information provided to Service Providers are advised to contact the particular Service Provider. Service Providers will be required to obtain written permission from applicants and participants in order to collect and use any additional information collected for purposes other than RT. (See Section 6.3)

Service Provider Personnel

Information collected on Service Providers' and their subcontractors' key personnel (as defined earlier) will be used to conduct fingerprint-based criminal history records checks and name-based security threat assessments.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as data mining)?

No. Please note that there may be other uses of other data by the Service Provider. The individual will have to consult their Service Provider for specific information; however, information collected for the purposes of the program must be limited to uses associated with the program.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

The information needed to conduct RT operations will be collected directly from the RT applicants by the Enrollment Provider. The individual will have the opportunity to review the information for accuracy before it is transmitted to TSA. As part of the annual RT membership renewal process, the Service Provider will ask individuals to review the information in their file and to confirm or update their records.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

It is expected that Enrollment Providers will collect accurate information from RT applicants by collecting directly from the individual and verifying the accuracy of that information. Only the "approved"

or "not approved" security threat assessment determinations are shared with service providers. TSA does not share the security threat assessment case history. Uses of the information are limited to identifying the individual, conducting and adjudicating a security threat assessment, and issuing an RT card.

The information collected under the program cannot be used by the service providers for non-program purposes unless the individual expressly authorizes the use (Opt In requirement). TSA enforces the restrictions on the use of the information as part of the standards for participation in the program.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

TSA will retain the data it receives in accordance with a record retention schedule that is currently being prepared and will be submitted to National Archives and Records Administration (NARA) for approval as described in Section 3.2.

TSA envisions that different retention policies will be established for different categories of individuals. TSA plans to propose that biographic and biometric data will be retained for at least six years from the date an individual's participation in the RT program ends. The record retention period will be defined in the applicable record retention schedule for security threat assessments that will be submitted to NARA for approval and published in the Federal Register by NARA.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

The applicable record retention schedule covering the security threat assessment portion of the RT process is currently being prepared by TSA and will be submitted to NARA for approval.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

Information collected through this program will be maintained in accordance with NARA-approved record retention schedules in furtherance of TSA's mission to ensure the security of the Nation's transportation system. Records will be retained for at least six years to permit judicial review in the event of litigation, as well as to reduce the incidence of fraudulent applications.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

The information TSA receives from individuals may be shared with DHS employees and contractors who have a need for the information in the performance of their duties, including but not limited to

immigration, law enforcement or intelligence operations. This information will be shared in accordance with the provisions of the Privacy Act, 5 U.S.C. § 552a.

In accordance with the Privacy Act, TSA may obtain an individual's express written consent to share that individual's biographic and/or biometric data with other DHS components to facilitate his or her enrollment in other biometric credentialing programs.

4.2 For each organization, what information is shared and for what purpose?

In the ordinary course, information will be retained and used within the Transportation Threat Assessment and Credentialing (TTAC) office. TSA will also ordinarily share information with DHS components, including components contacted in connection with conducting immigration checks. TSA may also share information about individuals posing or suspected of posing a threat to transportation or national security within DHS for intelligence, counterintelligence, law enforcement or other official purposes related to transportation security in accordance with the provisions of the Privacy Act, 5 U.S.C. §552a. TSA will share information about individuals with those DHS employees who need the information in the performance of their duties. For example, if an individual writes his/her Congressman, information may be shared with the Office of Legislative Affairs or Office of Chief Counsel.

In accordance with the Privacy Act, TSA may also obtain an individual's express written consent to share that individual's biographic and/or biometric data with other DHS components to facilitate his or her enrollment in other biometric credentialing programs.

4.3 How is the information transmitted or disclosed?

Depending on the specific situation and need, TSA may transmit this data with DHS employees and contractors who have a need for the information in the performance of their duties via data network, facsimile, paper format, telephonically, or in-person. The method of transmission and security safeguards may vary according to specific circumstances.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Information may be shared with DHS employees and contractors who have a need for the information in the performance of their duties in accordance with the Privacy Act. Privacy protections may include access controls, including passwords; real-time auditing that tracks access to electronic information; and mandated training for all TSA employees and contractors.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

After conducting a security threat assessment, TSA will utilize the CIMS to notify the Enrollment Provider of the "approved" or "not approved" security threat assessment determination for RT applicants.

TSA will not disclose the details of the security threat assessment to the CIMS, Sponsoring Entities or Enrollment Providers and will limit the dissemination of information to "approved" or "not approved" only.

The Enrollment Provider is responsible for informing the RT applicant of his or her acceptance in the program – usually in conjunction with issuing the RT card. If an RT applicant receives a ""not approved" security threat assessment, TSA will inform the applicant directly in addition to notifying the Service Provider via the CIMS. For an employee of the Service Provider, TSA will notify the individual and the entity that submitted the individual's data.

TSA may share RT applicant's, RT participant's or Service Provider (including subcontractors) key personnel's biographic and biometric information and security threat assessment information with the Terrorist Screening Center (TSC) and the agency that nominated the individual for placement on a watch list in order to resolve any potential or suspected matches to a terrorist watch list. TSA may also share information about individuals posing or suspected of posing a threat to transportation or national security outside of DHS, including with TSC or the nominating agency, for intelligence, counterintelligence, law enforcement or other official purposes related to transportation security in accordance with the provisions of the Privacy Act. In addition, TSA may share the information it receives with Federal, state, or local law enforcement or intelligence agencies or with the airport operator or other organizations in accordance with the routine uses identified in the applicable Privacy Act system of records notices (SORN), DHS/TSA 002, Transportation Security Threat Assessment System (T-STAS) and DHS/TSA 015, Registered Traveler Operations Files. DHS/TSA 002 was last published in the Federal Register on November 8, 2005 and can be found at 70 FR 67,731-67,735 and 70 FR 67,735-67,736. DHS/TSA 015 was last published in the Federal Register on November 8, 2005, 70 FR 67,731, 67,735.

Iris images may be shared with the National Institute of Standards and Technology (NIST) for the sole purpose of research to develop government technology standards for the use of iris images.

5.2 What information is shared and for what purpose?

TSA may share an individual's biographic and certain biometric information and security threat assessment information with the Terrorist Screening Center and the nominating agency to the extent necessary to resolve potential matches or to facilitate an operational response. TSA may share information about individuals posing or suspected of posing a threat to transportation or national security to entities outside of DHS, including TSC or the nominating agency, for intelligence, counterintelligence, law enforcement or other official purposes related to transportation or national security in accordance with the provisions of the Privacy Act and the applicable SORNs.

Participants may volunteer iris images by separate opt-in process to share images with NIST for the sole purpose of developing government technology standards for the use of iris images.. In such cases, iris images will be shared with the National Institute of Standards and Technology (NIST) only after TSA enters into a Memorandum of Understanding with NIST to minimize privacy impacts and secure the data.

5.3 How is the information transmitted or disclosed?

Depending on the specific situation and need, TSA may transmit this data within DHS only to those who need the information to perform their official duties via data network, facsimile, in paper format,

telephonically, or in person. The method of transmission and security safeguards may vary according to specific circumstances. Transmission of individual information between the Service Provider and CIMS, and between the CIMS and TSA is transmitted electronically and encrypted in transit.

Biographic and biometric information collected from an RT applicant by the Enrollment Provider is sent electronically by the Sponsoring Entity to the CIMS. The CIMS then sends the biographic information to TSA to conduct the security threat assessment. The CIMS aggregates, retains, and distributes information (on a needed basis) to the entities participating in 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, "approved / not approved" security threat assessment determinations, and other information as directed by the TSA. The TSA will require that all Service Providers participating in RT connect with the CIMS. The CIMS will be a commercially neutral entity, acting under contract to TSA, whose role is to support an open marketplace; the CIMS may not sell or disseminate any biographic and/or biometric data collected by Service Providers for RT. The CIMS will be primarily responsible for:

1. Receipt of enrollment information from the Enrollment Provider through the Sponsoring Entity;
2. Biometric storage;
3. Format and transfer of data required for TSA Security Threat Assessment;
4. Maintenance of participant and revocation databases;
5. Encryption and certification management;
6. Card payload creation; and
7. Fee pass through to TSA in accordance with the Registered Traveler Fee Notice, once that notice is issued.

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.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

Yes. TSA and Terrorist Screening Center (TSC) entered into an MOU on May 12, 2006. Information may be shared in accordance with the applicable SORNs, DHS/TSA 002 Transportation Security Threat Assessments, and DHS/TSA 015, Registered Traveler Operations, or in accordance with the provisions of the Privacy Act, 5 U.S.C. §552a.

In the event that TSA decides to share iris images with NIST for the purpose of developing government technology standards, an MOU will be prepared to provide privacy and security safeguards that will be consistent with the opt-in agreements engaged by individual RT participants.

5.5 How is the shared information secured by the recipient?

Any Federal agency receiving RT data is expected to handle the data in accordance with the Privacy Act, that agency's SORN(s) and FISMA. In addition, information received by the Service Providers must be protected against compromise through encryption technologies and physical security requirements established in the TSA-issued RT standards.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

None is required specific to this program; however, any Federal agency receiving this information is expected to handle it in accordance with the Privacy Act and that agency's SORN(s). Service Providers, Sponsoring Entities and the CIMS involved in the handling of personal data must develop and conduct training that comports with TSA-issued RT standards.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

TSA will share this information under the applicable provisions of the SORN and the Privacy Act. By limiting the sharing of this information and by ensuring that recipients properly handle the data, TSA is mitigating any attendant privacy risks.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, why not?

Yes. Consistent with 5 U.S.C. 552a(e)(3), TSA will mandate that the Enrollment Provider provide a Privacy Act Statement to RT applicants regarding the information collected. (See Appendix B for statement.) Because RT is a strictly voluntary program, consent is a prerequisite for participation in the program. The Privacy Act Statement will describe the authority for the collection of the information, the purpose for the collection of information, whether provision of the information is voluntary, and any consequences of failing to provide the requested information. Additionally, the Enrollment Provider will provide RT applicants with a copy of its written privacy policy. Individuals who choose not to apply or participate in RT can continue to fly commercially by undergoing normal airport security screening procedures.

Service Providers' key personnel involved in RT operations will be provided with a Privacy Act Statement at the time of collection of their biographic and biometric information that will describe the authority for the collection of the information, the purpose for the collection of the information, whether

provisions of the information is voluntary or mandatory, and the consequences of failing to provide the requested information. (See Appendix B for statement.)

6.2 Do individuals have an opportunity and/or right to decline to provide information?

While the RT program is strictly voluntary, any individual wishing to apply to be a participant in the program is asked to provide the personal information listed in section 1.1 in order for TSA to conduct a security threat assessment and enable biometric identity verification at the point security checkpoint. If the individual chooses not to provide all of the information requested, he or she may still apply for the program but TSA may not be able to conduct or complete a Security Threat Assessment, which is a requirement for enrollment in RT.

Service Provider's (including subcontractors) key personnel involved in RT operations will also be asked to provide the information provided to comport with TSA-issued RT standards. Provision of this information is voluntary. However, if those individuals do not wish to provide the information, it may delay or prevent an "approved" determination of the security threat assessment and criminal history records check necessary to work on Registered Traveler. Without an approved security threat assessment, that employee cannot be allowed to work on Registered Traveler. It may also impede or restrict the Service Provider from meeting TSA-standards which are required for participation in the RTIP.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

Yes. The applicant has the right to consent via opt-in if the Enrollment Provider seeks to collect any information beyond what is requested for enrollment in the RT program or use any information collected for purposes other than RT operations. The Enrollment Provider must inform the applicant or participant that the information is not required by TSA for participation in the RT program. In addition, individuals have the right to consent to use of iris images for research purposes.

Service Provider's (including subcontractors) key personnel do not have the right to consent to particular uses of their information.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

RT applicants and participants receive applicable privacy information before applying and must provide consent to have their information collected. Service Providers are informed of the personnel requirements and may elect whether to participate. Individual privacy concerns are mitigated by the voluntary nature of the entire program. Express consent from the individual is required before iris images may be used for research purposes.

Section 7.0 Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

Individuals may request access to their information by submitting a Freedom of Information Act/Privacy Act (FOIA/PA) request to TSA in writing by mail to the following address:

Transportation Security Administration, TSA-20, East Tower
FOIA Division
601 South 12th Street
Arlington, VA 22202-4220

FOIA/PA requests may also be submitted by fax at 571-227-1406 or by filling out the Customer Service Form (www.tsa.gov/public/contactus). The FOIA/PA request must contain the following information: Full Name, address and telephone number, and email address (optional). Please refer to the TSA FOIA web site (www.tsa.gov/public). In addition, individuals may amend their records through the redress process as explained in paragraph 7.2 below.

In the case of criminal history records checks, if a Service Provider employee disputes the results of a fingerprint-based criminal history records check (i.e., that the disposition of a charge (s) is incorrect), the applicant can provide court documentation to TSA. If the employee can show that the disposition (or charge) that the "not approved" result is based on inaccurate information, the determination will be changed to "approved."

Individuals who have been denied participation in the RT program by TSA will be given the opportunity to contact TSA to address their concerns. Redress based on the name-based portion of the security threat assessment will be handled on a case-by-case basis due to the classified and/or security sensitive information that may be involved. TSA will provide information on which portion of the assessment the determination was based to the applicant to the extent permitted by law. There may be items that are classified or sensitive security information that cannot be released. Individuals who believe that their immigration status check determination is inaccurate should contact Immigration and Customs Enforcement (ICE) to address their concerns and will have to contact TSA once their concerns are addressed by ICE.

7.2 What are the procedures for correcting erroneous information?

An individual may download redress information from the TSA public website at www.tsa.gov, contact the TSA at (866) 289-9673, or E-mail: TSA-ContactCenter@dhs.gov if delayed when checking in for a boarding pass due to TSA's watch list clearance procedures.

- TSA will send a Traveler Identity Verification Form (TIVF) to the individual or the individual may download the TIVF from the website or access the secure web-based portal and complete the form online.
- TSA requests that the applicant submit the completed TIVF to TSA at Transportation Security Administration, TSA-901, 601 South 12th Street, Arlington, VA 22202. Except in

the case of a minor, only the person seeking expedited watch list clearance procedures may submit the Traveler Identity Verification Form.

- TSA will review the submission and reach a determination of whether reconsideration of the "not approved" security threat assessment determination is warranted. During the redress process, it may be necessary for TSA to collect additional information from the individual in order to facilitate the redress process, including notarized copies of identification documents, such as a birth certificate or passport. If TSA needs additional information in order to continue the redress process, the individual will be notified in writing. The information requested will be the minimum necessary to complete the redress process.
- If redress results in an "approved" security threat assessment determination, TSA will notify the individual of that finding in writing and contact the appropriate parties, such as the CIMS and the Sponsoring Entity/Service Provider, to facilitate RT enrollment.

In addition to the redress process, the individual may also request correction of his or her records pursuant to the Privacy Act. While this system of records is subject to certain exemptions under the Privacy Act, TSA may amend its records when appropriate. Such requests should be sent to the address noted in section 7.1 above.

7.3 How are individuals notified of the procedures for correcting their information?

If the security threat assessment results in a "not approved" status, TSA will inform the individual directly by letter and notify the individual of the redress procedures. In addition, individuals are notified of the redress procedures by accessing the TSA public website at the web address listed above, contacting TSA at (866) 289-9673 or e-mail TSA-ContactCenter@dhs.gov by the air carriers at the airport.

7.4 If no redress is provided, are alternatives available?

A redress process is provided.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

Individuals may request access to or correction of their personal information pursuant to a redress process and an appeals process and pursuant to the Privacy Act consistent with exemptions contained in the system of records.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system?

In order to manage, upgrade and utilize the TSA system, system administrators, security administrators, IT specialists, vetting operators, analysts and other persons may have a need to access the TSA system or the information in the system in the performance of their duties. Role-based access controls are employed to limit the access of information by different users based on the need to know. TSA also employs processes to enforce separation of duties to prevent unauthorized disclosure or modification of information. No unauthorized users are permitted access to system resources. Strict adherence to access control policies is automatically enforced by the TSA system in coordination with and through oversight by TSA security officers.

8.2 Will contractors to DHS have access to the system?

Contractors who are hired to perform many of the IT maintenance and security monitoring tasks have access to the TSA system in order to perform their official duties. Strict adherence to access control policies is automatically enforced by the TSA system in coordination with and through oversight by TSA security officers. All contractors performing this work are subjected to Homeland Security Acquisition Regulation (HSAR) requirements for suitability and a background investigation.

8.3 Does the system use "roles" to assign privileges to users of the system?

Role-based access controls are used for controlling access to the TSA system using the policy of Least Privilege, which states that the TSA system will enforce the most restrictive set of rights/privileges or access needed by users based on their roles.

8.4 What procedures are in place to determine which users may access the system and are they documented?

The TSA system is secured against unauthorized access through the use of a layered, defense-in-depth security approach involving procedural and information security safeguards.

All TSA and DHS employees and assigned contractor staff receive DHS-mandatory privacy training on the use and disclosure of personal data. They also receive appropriate security training and have any necessary background investigations and/or security clearances for access to sensitive information or secured facilities based on TSA security policies and procedures.

All government and contractor personnel are vetted and approved for access to the facility where the TSA system is housed, issued picture badges with integrated proximity devices imbedded, and given specific access to areas necessary to perform their job function. A Rules of Behavior document provides an overall guidance of how employees are to protect their physical and technical environment and the data that is handled and processed. All new employees are required to read and sign a copy of the Rules of Behavior prior to getting access to the TSA system.

All personnel working in or accessing the TSA facility are required to wear a security office issued control badge with picture and name. The badges provide the electronic access control cards used to gain entrance to the secure area for the computer operations room. Badges must be worn and displayed at all times while on the premises.

Pursuant to the contract establishing the Central Information Management System (CIMS), TSA will require the CIMS system owner to establish procedures to govern access control to the CIMS that will meet or exceed TSA security standards. The security requirements would cover such things as how RT sensitive information is to be handled and protected at the contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), the background investigation and/or clearances required, and the facility security required. These requirements would cover information technology, hardware, software and the management operations, maintenance, programming, and system administration of computer systems, networks, and telecommunication systems.

TSA requires that data be handled in accordance with the Privacy Act of 1974 and the CIMS system will comply with FISMA requirements.

Sponsoring Entity and Service Provider systems that receive, store or transmit RT data will be required by TSA to comply with access control requirements established in TSA-issued RT standards. The Sponsoring Entities and Service Providers will need to document how their systems meet with the TSA-issued standards as part of a plan of operations submitted to TSA for review and approval before operations can begin.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Employees or contractors are assigned roles for accessing the TSA system based on job function. The Facility Security Officer and the Information System Security Officer coordinate to ensure compliance to policy, and manage the activation or deactivation of both physical and computer accounts and privileges as required or when expired. TSA ensures personnel accessing the TSA system have security training commensurate with their duties and responsibilities. All personnel are trained through TSA's Security and Awareness Training Program when they join the organization and periodically thereafter. The status of personnel who have completed the training is reported to TSA on a monthly basis.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

Pursuant to a contract with TSA, the CIMS must comply with the Privacy Act of 1974, 5 U.S.C. §552a, and FISMA to ensure the privacy and security of the data collected and submitted to TSA.

Except where the applicant/participant provides written consent, 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 retain an anonymous RT identification number, biometric information (needed to check for duplicate applications), renewal date, an "approved" or "not approved" Security Threat Assessment finding, and other information as directed by TSA.

The TSA and CIMS systems are audited annually by the TSA IT Security Office and will include a real-time audit trail to:

1. Track access to electronic information and changes to data;
2. Monitor implementation and use of intrusion detection software and hardware;
3. Verify installation of data integrity monitoring software;
4. Provide real time monitoring of TSA and CIMS system audit logs; and
5. Ensure separation of data access based on user roles and responsibilities.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All government and government-contractor personnel are required to complete TSA Privacy Training. Compliance with this requirement is audited monthly by the TSA Privacy Officer. In addition, regular security training is provided to raise the level of awareness for protecting and processing personal information. TSA does not provide privacy training to the Enrollment or Service Providers, but does require those entities to develop and conduct privacy training.

Enrollment Provider personnel and their contractors who collect and maintain RT Applicants' and Participants' personal information must be properly trained, have "approved" security threat assessments, and comply with TSA standards regarding having their own privacy policy. 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. Before Service Provider personnel are allowed to collect and use RT applicant and participant information, the Service Provider must demonstrate that it meets TSA-issued RT standards.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Information in TSA's record systems is safeguarded in accordance with FISMA, which establishes government-wide computer security and training standards for all persons associated with the management and operation of Federal computer systems.

TSA Office of the Chief Information Security Officer (OCISO) Audit Program staff will perform scheduled and ad-hoc assessments of the RT program, including Sponsoring Entity/Service Provider IT systems, as part of ongoing assessments the OCISO performs for systems that house RT applicant and participant data. These assessments review Sponsoring Entity/Service Provider IT system practices and operations to determine the effectiveness of the systems technical, operational and managerial security controls. The baseline security requirements used for the assessments are derived from those FISMA sections deemed appropriate for application to Sponsoring Entity/Service Provider systems. Certification and Accreditation (C&A) for the CIMS will be completed before operating. C&A for the system was completed August 11, 2006.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Data on the TSA and CIMS systems is secured in accordance with applicable Federal standards. Security controls are in place to protect the confidentiality, availability, and integrity of personal data, including role-based access controls that enforce a strict need to know policy. Physical access to the system is strictly controlled with the use of proximity badges and biometrics. The TSA system is housed in a controlled computer center within a secure facility. In addition, administrative controls, such as periodic monitoring of logs and accounts, help to prevent and/or discover unauthorized access. Audit logs are maintained and monitored to track user access and unauthorized access attempts. Each airport or air carrier will include a provision in its contract with its Service Provider authorizing TSA oversight. Oversight may include (but is not limited to) announced, unannounced, and or unscheduled inspections. Failure to comply with RT Standards or to cooperate with TSA or its contractors will be considered by TSA in decisions regarding the ongoing participation in RT. In addition, in order to be deemed eligible to participate in the RT program, Service Providers must meet stringent TSA criteria for maintaining the privacy and security of all RT data, which are based on the NIST standards 800-53 and Federal Information Processing Standards (FIPS) 199. By requiring the Service Providers to meet these criteria, TSA minimizes any attendant privacy risks associated with the handling of RT information by the non-Federal entities that are not subject to Federal IT security and privacy laws, regulations and policies.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

The TSA system is primarily built from Commercial Off the Shelf (COTS) products. TSA system components include COTS hardware and operating systems. This system was provided to TSA from the Department of Transportation upon TSA stand-up.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

RT is designed to allow for collection of only those data elements necessary to allow TSA and the Sponsoring Entities to complete their tasks. Additional information is only requested as needed and in the vast majority of cases, a limited initial set of information will be sufficient to resolve adjudication questions related to the security threat assessment.

9.3 What design choices were made to enhance privacy?

In order to support privacy protections, TSA has developed an information technology infrastructure that will protect against inadvertent use of personally identifying information. Access to data collected for this program will be strictly controlled- only TSA employees and contractors with proper security credentials and passwords will have permission to use this information. TSA will not transmit or otherwise share this information with entities outside of DHS that are not described in the routine uses in

the applicable SORNs, DHS/TSA 002, Transportation Security Threat Assessments, and DHS/TSA 015, Registered Traveler Operations, or with other agencies as may required pursuant to the Privacy Act. Additionally, the TSA and CIMS systems will include a real time audit function to track access to electronic information, and any infraction of information security rules will be dealt with quickly and appropriately. All TSA and assigned contractor staff receive TSA-mandated privacy training on the use and disclosure of personal data. The procedures and policies in place are intended to ensure that no unauthorized access to records occurs and that operational safeguards are firmly in place to prevent system abuses.

Only minimal information is stored on the RT card. The card contains only enough biometric data, stored within an applet on the card, to confirm a person's identity when he or she travels. Biometric data will be associated with a unique identifier to confirm that the traveler is an active RT participant. As a safeguard against biometric theft, fingerprints are not stored on the RT card as an image, but as a template which prevents unauthorized parties from replicating the biometric. Also, Service Providers may add additional information to the card but cannot add information to the RT program applet on the card or access or utilize the information on that applet for purposes other than RT.

9.4 Privacy Impact Analysis:

These conscious design choices will limit access to the personal information, thereby mitigating any possible privacy risks associated with this program. Information received from the applicant is limited to data needed to operate the program, including facilitating adjudication to resolve potential matches without the delay and cost associated with requesting additional information from the applicant. The RT Interoperability Consortium requires that Service Provider privacy policies be at least as stringent as TSA's, but permits policies that are more stringent.

Conclusion

Registered Traveler is designed to restrict access to and use of personal information based on program need. Due to its structure as a private sector program facilitated and overseen by TSA, Registered Traveler has complexity in the collection, storage and transmission of personal data. TSA consequently has necessary safeguards to protect personal information and requires that private sector Sponsoring Entities and Service Providers provide the public with its privacy policies. As TSA undergoes rulemaking to establish a national RT program, the public will have further opportunities to provide comments and make recommendations regarding privacy.

Responsible Officials

John Martinez

Office of Transportation Threat Assessment & Credentialing

Transportation Security Administration

Arlington, VA 22202

Registered.Traveler@dhs.gov

Approval Signature Page

_____

Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration

_____

Hugo Teufel III

Chief Privacy Officer
Department of Homeland Security

Appendix A

Eligibility Requirements

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.

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 and must consent in writing to permit the child to join RT.

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[1] and 2) Verification Providers to provide verification services at RT Kiosks.

RT Applicants must be able to receive and maintain an "approved" Security Threat Assessment determination.

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.

[1] Security Threat Assessments are TSA-conducted checks against Government databases to determine eligibility for RT. See Section 1.3 for more information.

Appendix B

Registered Traveler Privacy Act Statements

For applicants:
TSA Privacy Act Statement

Authority: 49 U.S.C. 114 authorizes collection of this information.

Purpose: TSA is collecting this information from all individuals who apply to participate in the Registered Traveler program. TSA will use this information to verify your identity, to conduct and adjudicate a security threat assessment, and, if you are accepted into Registered Traveler, to conduct ongoing security threat assessments and to issue a "smart card" to you that will identify you as a Registered Traveler. Furnishing this information, including the Social Security number, is voluntary. However, failure to provide it may delay or prevent the completion of the security threat assessment, without which you may not be permitted to participate in this program.

Routine Uses: The information will be used by and disclosed to TSA personnel and contractors or other agents who need the information to assist in the operation of Registered Traveler. Additionally, TSA may share this information with airports and airlines to the extent necessary to ensure proper identification, ticketing, security screening, and boarding of Registered Travelers. TSA may disclose information to appropriate law enforcement or other government agencies as necessary to identify and respond to outstanding criminal warrants or potential threats to transportation security. TSA may also disclose information pursuant to its published system of records notices, DHS/TSA 002, Transportation Security Threat Assessment System (T-STAS) and DHS/TSA 015, Registered Traveler Operations Files, both of which were last published in the Federal Register on November 8, 2005, at 70 FR 67731-67736.

.

For Service Providers' key personnel:
TSA Privacy Act Statement

Authority: 49 U.S.C. 114 authorizes collection of this information.

Purpose: TSA is collecting this information from all Registered Traveler (RT) Service Provider (including subcontractors) key personnel. You are provide personal information necessary to conduct a fingerprint-based criminal history records check and a name-based security threat assessment to determine whether you meet requirements set forth in TSA-issued Registered Traveler standards and whether you pose or are suspected of posing a threat to transportation or national security. Key personnel for Service Provider (including subcontractors) are defined as: 1) officers, principals, and program managers responsible for RT operations; and 2) all employees that collect, handle or use RT applicant or participant data. Furnishing this information is voluntary and you may decline to provide all or part of the requested biographic or biometric information. However, if you do not provide the information, it may delay or prevent an "approved" determination of the security threat assessment and criminal history records check necessary to work on Registered Traveler. In such instances, you would not be allowed to work on Registered Traveler and it may impede or restrict the Service Provider from meeting TSA-standards which are required for participation in the RTIP.

.

Routine Uses: The information will be used by and disclosed to TSA personnel and contractors or other agents who need the information to assist in the operation of Registered Traveler.

Additionally, TSA may share this information with airports and airlines to the extent necessary to ensure proper compliance with TSA-issued Registered Traveler standards. TSA may disclose information to appropriate law enforcement or other government agencies as necessary to identify and respond to outstanding criminal warrants or potential threats to transportation security. TSA may also disclose information pursuant to its published system of records notice, DHS/TSA 002, Transportation Security Threat Assessment System, which was last published in the Federal Register on November 8, 2005 and can be found at 70 FR 67731-67735.