Transportation Security Administration

Registered Traveler Pilot

Privacy Impact Assessment

June 24, 2004

Contact Point:

Lisa S. Dean
Privacy Officer
Transportation Security Administration
571.227.3947

Reviewing Official:

Nuala O'Connor Kelly
Chief Privacy Officer
U.S. Department of Homeland Security
202.772.9848

I. Introduction

The Aviation and Transportation Security Act (ATSA), P.L. 107-71, Section 109 (a)(3) authorizes the Transportation Security Administration 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, TSA proposes to conduct a Registered Traveler (RT) Pilot Program in a limited number of airports to test and evaluate the merits of this type of trusted passenger program.

Under the Registered Traveler Program as envisioned by TSA, qualified travelers will be positively identified via advanced identification technologies in order to confirm that these travelers are not suspected of posing a threat to aviation security. The RT pilot will collect biographical information and a biometric from airline passengers who volunteer to submit to a security threat assessment, which will include checking their identities against terrorist-related databases and appropriate criminal databases for outstanding warrants. If an RT volunteer passes the security threat assessment, TSA will use their biometric information to verify their identity when they present themselves for screening at the airport security checkpoint. This should expedite the screening of registered travelers and allow TSA to focus its security efforts more appropriately.

This Privacy Impact Assessment (PIA), conducted pursuant to 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, is based on the current design of the program and the Privacy Act system of records notice, Registered Traveler Operations Files (DHS/TSA 015), that was published in the Federal Register on June 1, 2004. This PIA provides further details about the collection of personally identifiable information for the purpose of conducting security threat assessments and issuing an RT card during the pilot.

II. System Overview

- **What information will be collected and used for this security threat assessment?**

An important part of the information collected for the security threat assessment for the RT pilot is the fact that participation will be strictly voluntary. Accordingly, if individuals are concerned about the privacy implications of providing their personal data, they simply need not participate in the program. Individuals who choose to participate in the pilot will provide the information listed below, which will be used by TSA to complete a name-based security threat assessment prior to acceptance of the volunteer as a registered traveler: full name, social security number, other names used, home address, home telephone number, cell phone number, email address, date of birth, place of birth, nationality, gender, prior addresses (for the past five years), drivers license number, and biometric identifiers (fingerprints and/or iris scan).[1] E-mail information is used for identity verification as well to contact volunteers concerning their enrollment status.[2] If the volunteer has no email address, they can call the hotline to verify status.

- **Why is the information being collected and who is affected by the collection of the data?**

The information is being collected from volunteers for the RT pilot in order to perform a name-based security threat assessment of individuals who volunteer for the RT pilot program and to issue an RT card linked to the volunteer's biometric information. As explained above, TSA

[1] TSA will collect two fingerprints and an iris scan of both eyes at enrollment.

[2] For the program itself, email addresses will be used by TSA to keep customers informed of any changes that might occur with regard to the agency's privacy policies and/or the Privacy Impact Assessment governing this program.

collects and uses the biometric data to verify the identity of Registered Travelers at the airport security checkpoint.

Information gathered from volunteers for the RT pilot will be used for the following purposes:

(1) To pre-screen and positively identify low-risk travelers by conducting security threat assessments and using advanced identification technologies, including biometrics, to expedite passengers' security screening at airport checkpoints,

(2) To identify individuals impersonating law enforcement officers who attempt to board commercial aircraft while armed;

(3) To assist in the management and tracking of applicant and member security assessments;

(4) To permit the retrieval of the results of security assessments, including criminal history records checks and searches in other governmental identification systems, performed on volunteers;

(5) To refer to the appropriate intelligence and law enforcement entities the identity of volunteers who pose or are suspected of posing a security threat with the appropriate intelligence and law enforcement entities.

- **What are the specifics of the program, paying particular attention to the collection and use of biometrics?**

TSA will collect biographical and biometric information directly from the passengers who are enrolling in the RT pilot program at the airport enrollment station. Once the enrollment is completed each Registered Traveler candidate will be issued a member card with his or her biometrics encrypted and encoded on it. Biometrics will only be used for purposes of identity verification. The card will not be activated unless and until a candidate completes a security threat assessment and TSA has determined that they are not suspected of posing a security threat. TSA employees and a government contractor specifically hired for the purpose of collecting and securing the data will collect and maintain this information in accordance with the Privacy Act systems of record notice for the RT Pilot (DHS/TSA 015).

Information will be collected at enrollment stations in the airport where the volunteer applies. During enrollment, the information will be securely stored and password-protected on desktop/laptop computers. All biographical data will be downloaded via encrypted removable media (CD, memory stick) to a TSA computer connected to the secure TSA network. The biometric information collected will be used only to verify identification and enrollment in the program at the Registered Traveler security checkpoint. Biometrics will only be stored on the individual's member card and in the Registered Traveler database at the pilot location. Biometrics will not be used to conduct security threat assessments.

The biographical information will be used to conduct a security threat assessment by running the names and biographic information through terrorist-related and appropriate criminal databases. If any individual whose name and other biographic data submitted appears to meet the minimum criteria established by the database as a possible match, that information will be forwarded to TSA for further screening, and a determination that the individual does not pose or is not suspected of posing a security threat. After TSA review, the name of any passenger posing or suspected of posing a security threat will be forwarded to appropriate law enforcement and/or intelligence agency(ies) for either action or further investigation. The purpose for adding a further review by TSA of potential matches is to add a layer of protection for those individuals who may be affected by the threat assessment process and to reduce as much as possible the number of "false positives" that may affect individuals whose names are submitted for the program. All

volunteers will receive a card containing their biometric. However, volunteers are not considered enrolled in the RT pilot program until they have cleared a security threat assessment.

TSA will transmit to the contractor, via secure email, the names of those volunteers who have cleared the security threat assessment. The contractor will encrypt the data about Registered Travelers onto removable media and manually transfer the data to their secure desktop/laptop computers at the airport enrollment and security checkpoint stations. In addition, the contractor will send an e-mail to the applicant, via the e-mail account provided at enrollment, informing the traveler of his/her status in the program; either accepted or rejected. At the airport participants will present their member card to TSA contractors at a kiosk set up at the RT screening checkpoint. The participant's biometric information will be matched to the card for identity verification. The system will check the individual's identity against the status of his or her security threat assessment at which time the system will allow verified participants to proceed through the security checkpoint. Any participant whose biometric cannot be matched or threat assessment verified at the Registered Traveler security checkpoint will be directed to the regular security checkpoint lines.

In the case where the airport operates on a card-less system, the Registered Traveler will simply submit his or her biometrics at the checkpoint to be matched to the biometrics captured at enrollment and stored in the Registered Traveler Database on site. The system will check the individual's identity against the status of his or her security threat assessment at which time the system will allow verified participants to proceed through the security checkpoint. Any participant whose biometric cannot be matched or threat assessment verified at the Registered Traveler security checkpoint will be directed to the regular security checkpoint lines. In all cases names will be periodically run against the terrorist and criminal databases throughout the course of the pilot program in order to ensure that all enrollees remain eligible. This pilot program will not supplant regular screening procedures and enrollees remain subject to routine passenger screening at airport security checkpoints.

Volunteers whose identities match or potentially match an entry on a terrorist related databases cannot be eligible for the RT program. In this circumstance a transmittal will be sent in the same manner as above but will indicate that the volunteer is ineligible for the RT program. A transmittal will be sent in the same manner described above except it will indicate that a volunteer is not an acceptable candidate for the RT program. Volunteers biographical and biometric information will be maintained in the system whether or not they receive the RT credential. Additionally, if TSA makes a determination during the security threat assessment that a volunteer poses or is suspected of posing a security threat, TSA will share information about such volunteer with the appropriate law enforcement and/or intelligence agencies. All volunteers may find out if they have been granted RT status by calling a TSA hotline established at each RT pilot location. Additionally, all volunteers will be notified by e-mail of their status automatically when their security threat assessment has been completed. All biometric data will be stored on the contractor's database that will be secured and maintained in a secure/locked location by the contractor for the duration of the contract. In addition, biometric data will also be stored on the RT cards (ICC or 2D Bar Codes) provided to eligible Registered Travelers.

The biometric technology used in this pilot meets all National Institute of Standards and Technology, American National Standards Institute, Federal Information Processing Standards and Government Smart Card standards. The equipment was evaluated and tested using a live demonstration during contractor briefings and has been evaluated by the biometrics coordinator at TSA and DHS.

- **What notice or opportunities for consent are provided to individuals regarding what information is collected, and how that information is shared?**

Because RT is a strictly voluntary program, consent is a prerequisite for participation in the program. The RT application material will include a notice as required by the Privacy Act, 5

U.S.C. 552a(e)(3). The notice will describe the reasons for the collection of information, the consequences of failing to provide the requested information, and explain how the information will be used. Individuals who choose not to apply or participate in the program will continue to undergo normal airport security screening procedures.

The collection, maintenance, and disclosure of information will be in compliance with the Privacy Act and the published system of records notice for the RT pilot, DHS/TSA 015. Information about volunteers will be shared with TSA employees and contractors who have a "need to know" for implementation of the RT pilot and the SORN reflects the appropriate routine uses for disclosure of this information to the contractor. The contractors are contractually obligated to comply with the Privacy Act in their handling, use, and dissemination of personal information. As stated earlier, if TSA determines during the threat assessment that an applicant may pose or is suspected of posing a security threat, TSA will notify the appropriate law enforcement and/or intelligence agencies.

- **Does this program create a new system of records under the Privacy Act?**

Yes. The Registered Traveler (RT) Operations Files system of records notice was published in the Federal Register on June 1, 2004, and can be found at 69 Fed Reg. 30948, 30950.

- **What is the intended use of the information collected?**

The biometric information being collected will be used to establish a RT participant's identity. The biographical information will be used to conduct a security threat assessment by means of query against terrorist and criminal databases.

- **Will the information collected be used for any purpose other than the one intended?**

  Information collected will be used only for the purposes outlined, consistent with the Privacy Act of 1974 and the published system of records notice for the RT pilot, DHS/TSA 015. Specifically 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 the Registered Traveler pilot; to airports and airlines to the extent necessary to ensure proper identification, ticketing, security screening, and boarding of Registered Travelers; and to appropriate law enforcement or other government agencies as necessary to identify and respond to outstanding criminal warrants or potential threats to transportation security. See Attachment A, DHS/TSA 015 system of records notice for the RT program published June 1, 2004.

- **How will the information be secured against unauthorized use? (What technological mechanism will be used to ensure security against hackers or malicious intent?)**

TSA will secure personal information against unauthorized use through the use of a layered security approach involving procedural and information security safeguards. The data will be encrypted using National Institute of Science and Technology (NIST) and Federal Information Security Management Act (FISMA) standards and industry best practices when being transferred between secure workstations. Only TSA employees and contractors with proper security credentials and passwords will have access to this information to conduct the security threat assessment and identity verification at airport security checkpoints. Moreover, all TSA and assigned contractor staff receive DHS-mandated privacy training on the use and disclosure of personal data.

Specific privacy safeguards can be categorized by the following means, which are described in greater detail elsewhere in this document:

  - Technical limitations on, and tracking of, data access and use;

- Use of secure telecommunications techniques; and
- Limitation of physical access to system databases and workstations.

This approach protects the information in accordance with the following requirements:

The Privacy Act of 1974, as amended (5 USC 552a), which affords individuals the right to privacy in records that are maintained and used by Federal agencies.

Federal Information Security Management Act of 2002, (Public Law 107-347), which establishes minimum security practices for Federal security systems.

- **Will the information be retained and, if so, for what period of time?**

  TSA intends to retain these records for a sufficient period of time to conduct and review this pilot program. TSA does not yet have a record retention schedule approved by the National Archives and Records Administration (NARA) for records pertaining to this program and must retain these records until such schedule is approved. TSA is in the process of developing a records retention schedule that will dictate the retention period for these records. Once the records schedule is approved, TSA will amend this document to include the retention period for these records.

- **How will the applicant be able to seek redress?**

Enrollees who are identified as posing or suspected of posing a security threat will not be allowed to attain RT status. Due to the short duration of the RT pilot, RT volunteers who believe that they have been wrongly identified as a security threat will not be given the opportunity to appeal or seek other redress. Should the RT Pilot become a fully operational program, however, TSA will develop redress procedures for individuals who seek to participate in the program.

- **What databases will the names be run against?**

TSA will run the names against terrorist-related databases, and appropriate criminal databases for outstanding warrants, to determine if an individual poses or is suspected of posing a potential threat to aviation security

- **Step by step process of how the systems will work once the data has been input and what is the process for generating a response?**

All information will be collected manually from the individuals enrolling in the pilot program via electronic forms at the RT pilot site by the TSA employees or through a TSA contractor. The TSA employees or contractor will encrypt the data and forward it to TSA personnel. TSA will conduct the security threat assessment by running the names against terrorist related and appropriate criminal databases. The results of the checks are reviewed by TSA personnel for accuracy. TSA will further vet persons identified as potential matches against additional databases to further determine accuracy. Any individuals that TSA determines pose or are suspected of posing a security threat will not be awarded an RT credential and TSA will refer the identity of the individual to the appropriate law enforcement and/or intelligence agencies. Once eligible participants are identified, the data is encrypted and sent back to the contractor, who will load the information on their workstations at the respective RT site to activate the credentials of eligible enrollees. Each time a volunteer offers his RT card at an RT pilot location, the identity of the volunteer is authenticated by verifying that the biometric on the card matches the individual's biometric at the screening checkpoint.

- **What technical safeguards are in place to secure the data?**

Information in TSA's system is safeguarded in accordance with the Federal Information Security Management Act of 2002, (Public Law 107-347), which established government-wide computer security and training standards for all persons associated with the management and operation of Federal computer systems. Additionally, the system is managed in accordance with applicable TSA and DHS automated systems-security and access policies. The computer system from which records could be accessed is policy-and security-based; access is limited through user identification and password protection to those individuals who require it to perform their official duties. All data transferred on memory sticks is encrypted for security. The system also maintains a real-time auditing function of individuals who access the system. Databases that store personal information at the RT airport locations are housed on removable hard drives and will be stored in secured and locked facilities and containers in accordance with federal requirements.

TSA employs the following technical safeguards to secure data:

- Use of advanced encryption technology to prevent internal and external tampering of data and transmissions.
- Secure data transmission including the use of password-protected e-mail for sending files between the security threat assessment participants to prevent unauthorized internal and external access.
- Password protection for files containing personal or security threat assessment data to prevent unauthorized internal and external access.
- Network firewalls to prevent intrusion into DHS network and TSA databases.
- User identification and password authentication to prevent access to security threat assessment systems by unauthorized users.
- Security auditing tools to identify the source of failed TSA system access attempts by unauthorized users and the improper use of data by authorized operators.

Privacy Threats and Mitigation Measures

The table below provides an overview of the privacy risks associated with RT and the types of mitigation measures that address those risks.

Table 1: Overview of Privacy Threats and Mitigation Measures

Type of Threat	Description of Threat	Type of Measures to Counter/Mitigate Threat

Unintentional threats from insiders[3]	Unintentional threats include flaws in privacy policy definition; mistakes in information system design, development, integration, configuration, and operation; and errors made by custodians (i.e., personnel of organizations with custody of the information). These threats can be physical (e.g., leaving documents in plain view) or electronic in nature. These threats can result in insiders being granted access to information for which they are not authorized or not consistent with their responsibilities.	These threats are addressed by (a) developing a privacy policy consistent with Fair Information Practices, laws, regulations, and OMB guidance; (b) defining appropriate functional and interface requirements; developing, integrating, and configuring the system in accordance with those requirements and best security practices; and testing and validating the system against those requirements; and (c) providing clear operating instructions and training to users and system administrators.
Intentional threat from insiders	Threat actions can be characterized as improper use of authorized capabilities (e.g., browsing, removing information from trash) and circumvention of controls to take unauthorized actions (e.g., removing data from a workstation that has been not been shut off).	These threats are addressed by a combination of technical safeguards (e.g., access control, auditing, and anomaly detection) and administrative safeguards (e.g., procedures, training).
Intentional and unintentional threats from authorized external entities	Intentional: Threat actions can be characterized as improper use of authorized capabilities (e.g., misuse of information) and circumvention of controls to take unauthorized actions (e.g., unauthorized access to systems). Unintentional: Flaws in privacy policy definition; mistakes in information system design, development, integration, configuration, and operation; and errors made by custodians	These threats are addressed by technical safeguards (in particular, boundary controls such as firewalls) and administrative safeguards in the form of routine use agreements which require external entities (a) to conform with the rules of behavior and (b) to provide safeguards consistent with, or more stringent than, those of the system or program.
Intentional threats from external unauthorized entities	Threat actions can be characterized by mechanism: physical attack (e.g., theft of equipment), electronic attack (e.g., hacking, interception of communications), and personnel attack (e.g., social engineering).	These threats are addressed by physical safeguards, boundary controls at external interfaces, technical safeguards (e.g., identification and authentication, encrypted communications), and clear operating instructions and training for users and system administrators.

- **Will the staff working with the data have appropriate training and security clearances to handle the sensitivity of the information?**

All TSA and DHS and assigned contractor staff receive DHS-mandated privacy training on the use and disclosure of personal data. Staff assigned to handle classified information will be required to obtain appropriate security clearances.

Additionally, all staff must hold appropriate credentials for physical access to the sites housing the security threat assessment databases and management applications. Physical access safeguards include the use of armed or unarmed security guards at sites; hard-bolting or fastening of databases, servers, and workstations; and credential readers for internal and

[3] Here, the term "insider" is intended to include individuals acting under the authority of the system owner or program manager. These include users, system administrators, maintenance personnel, and others authorized for physical access to system components.

external site access. The TSA and DHS contractor also holds appropriate facility security clearances.

For questions or comments, please contact:

Lisa S. Dean, Privacy Officer, Transportation Security Administration, 571-227-3947

Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security, 202-772-9848