Transportation Security Administration

Registered Traveler Pilot (Private Sector Subpilot)

Privacy Impact Assessment

June 20, 2005

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. Overview

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, as described in its Privacy Impact Assessment of June 24, 2004, TSA conducts 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 Pilot Program, qualified travelers are 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 collects biographical information and biometric data from airline passengers who volunteer to submit to a security threat assessment. The security threat assessment includes checking volunteers' identities against terrorist-related databases and appropriate government databases for outstanding warrants. If an RT volunteer passes the security threat assessment, TSA uses their biometric information to verify their identity when they present themselves for screening at the airport security checkpoint. This process should expedite the screening of Registered Travelers and allow TSA to focus its security efforts among passengers more according to potential risk.

Because of the success of the Registered Traveler Pilot Program, TSA is now exploring the feasibility of applying the RT concept to a modified model that uses a Private Sector Partner. A Private Sector Partner may include airport authorities, air carriers, or other entities designated by TSA. To test the proposed model, TSA is launching a sub-pilot program known as the Private Sector Known Traveler (PSKT) in conjunction with the Greater Orlando Aviation Authority (GOAA).

This Privacy Impact Assessment (PIA) is an updated and amended version of the PIA that TSA issued on June 24, 2004. TSA has entered into an agreement to conduct a PSKT subpilot which will revise the operation of the program and TSA's role. PSKT is designed to have a structure that is very similar to the other pilots in the Registered Traveler Pilot Program. PSKT contains the same requirements for applicants, including 1) submitting biographic information to TSA for TSA to complete a security threat assessment; 2) submitting biometrics (fingerprint and iris data); 3) linking the security threat assessment to the volunteer's biometric information; and 4) verifying the identity of an enrollee at the airport security checkpoint. All participants in PSKT, referred to as "Known Travelers" or "KT," will be afforded the same expedited checkpoint screening and processing that is accorded for Registered Travelers in other RT pilots.

The difference between PSKT and the other RT pilots centers on the division of responsibilities between TSA and its Private Sector Partner. TSA's role will focus on conducting the initial threat assessment and periodic reassessments, as well as providing

standards, threat assessment screening, and oversight. To leverage the business processes of the private sector, the Private Sector Partner will have responsibility for procurement, operational, and marketing functions consistent with TSA guidelines.

Under PSKT, the Private Sector Partner invites volunteers to participate. Enrollment must be voluntary and is not a precondition for flying commercially. Eligible candidates must be US citizens, nationals of the United States, or lawful permanent residents and meet any other eligibility requirements stipulated by TSA and the Private Sector Partner.

The Private Sector Partner collects, from the KT applicant, his or her pertinent biographic and biometric information and sends it to TSA to conduct the security threat assessment. This assessment includes a check against the TSA's terrorist watchlists drawn from the Terrorist Screening Data Base (TSDB) maintained by the Terrorist Screening Center (TSC), against outstanding wants and warrants, and against other sources that TSA stipulates. All pilot participants (Registered Travelers and Known Travelers) undergo the same security threat assessment processes. Once TSA completes the security threat assessment, the agency will inform the Private Sector Partner whether the KT applicant has been accepted. The Private Sector Partner will inform the individual KT applicant of the outcome.

After review of the experience with this and other RT pilots and prior to implementation of the final program, TSA will issue a new PIA informing the public of changes to the program and any resultant impact to personal privacy.

II. System Overview

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

TSA will not collect the information needed to conduct the security threat assessment from the KT applicants directly. Such information will be collected by Private Sector Partner through its agent. With the express permission of KT applicants, the Private Sector Partner will collect biographic or biometric information to use for threat assessments.

An important facet of the PSKT program is 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.

KT applicants will provide the information listed below to the Private Sector Partner. Biographical information may include: full name, social security number[1] or alien registration information (if applicable), 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), driver's license number, and physical

1 The applicant also has the option of providing his (or her) Social Security number to facilitate the threat assessment process. A decision not to supply Social Security number or other biographic information may delay or prevent the completion of the security assessment, without which the applicant may not be permitted to participate in this program.

description. Biometric identifiers to be collected include fingerprints and a photograph of the iris.[2] E-mail information is used to contact KT applicants concerning their enrollment status or major changes to the program.[3] TSA will use this information to complete a name-based security threat assessment prior to acceptance of the KT applicant as a Known Traveler.

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

The information is being collected from applicants in order to perform a name- based security threat assessment and to issue them a KT card linked to their biometric information if they are accepted. As explained above, TSA requires that biometric data be used to verify the identity of Known Travelers at the airport security checkpoint.

Information gathered from volunteers for participation in the KT pilot will be used for the following purposes:

(1) To pre-screen and positively identify low-risk travelers by conducting security threat assessments and to accept them

(2) To expedite security screening at airport checkpoints for accepted Known Travelers by using advanced identification technologies, including biometrics;

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

(4) To permit the retrieval of the results of security assessments, including searches in governmental databases, performed on volunteers; and

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

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

A) Enrollment

The Private Sector Partner will collect biographical and biometric information directly from the KT applicants who are enrolling in the PSKT pilot program at the airport or other enrollment stations. The biometric technology used in this pilot meets all applicable National Institute of Standards and Technology, American National Standards Institute, Federal Information Processing Standards and Government Smart Card standards.

2 Additionally, the Private Sector Partner will collect ten fingerprints and an iris photo of both eyes at enrollment. TSA requires the Private Sector Partner to collect this information in order for the Private Sector Partner to verify participants' identity when seeking expedited travel as a KT and to conduct the threat assessment.

3 For the program itself, email addresses will be used by TSA or its Private Sector Partner to keep customers informed of changes that might occur with regard to the agency's privacy policies and/or the Privacy Impact Assessment governing this program and/or for other operational reasons.

Documents provided by the enrollee for personal identity verification will be scanned, authenticated and stored by the Private Sector Partner in accordance with their Privacy and Fair Information Practices and policies.

Once the enrollment is completed, the Private Sector Partner may choose to issue an inactive KT card to the applicant with his or her biometrics encrypted and encoded on it. If the candidate receives the card in advance of passing the security threat assessment and being accepted into the program, the card is inactive at the time of issuance and cannot be used to access KT privileges until activated. The KT card will not be activated unless and until a candidate completes a security threat assessment and TSA has determined that said candidates are not suspected of posing a threat to aviation security. If the Private Sector Partner chooses to issue the card after the threat assessment is complete and the candidate is accepted into the program, the Private Sector Partner may deliver the card by mail, by pick up, or by another approved delivery channel.

The Private Sector Partner's duly trained staff or contractors will collect and maintain this information in accordance with the Privacy Act systems of record notice for the RT Pilot (DHS/TSA 015). All biometric data will be stored on the Private Sector Partner's database that will be secured and maintained in a secure/locked location by the contractor for the duration of the contract. In addition, select biometric data necessary for operations will also be stored on the KT Integrated Circuit Chip cards (ICC) provided to eligible Known Travelers. During enrollment, the KT applicant's information will be securely stored and password-protected on desktop/laptop computers by the Private Sector Partner. All biographical data will be downloaded via encrypted removable media (e.g., CD or memory stick) to a TSA computer connected to the secure TSA network. Biometrics will be stored in encrypted fashion on the individual's member card, in the Registered Traveler database at the pilot location and at TSA or TSA's designated agent.

All biometric information collected will only be used to verify identification and enrollment in the program at the Registered Traveler security checkpoint. Biometrics will not be used to conduct security threat assessments.

The biographical information will be used to conduct a security threat assessment by comparing the names and biographic information to terrorist-related and appropriate criminal databases. In conducting the threat assessment, information will be stored and distributed to the vetting platforms and adjudication center by TSA using the Gateway Infrastructure maintained by the TSA Office of Transportation Vetting and Credentialing (OTVC).[4]

If a KT applicant's name and other submitted biographic data appear to meet the minimum criteria as a possible match, TSA will be notified for further action. TSA will then review the information and make a determination whether the individual poses or is

[4] See OTVC Screening Gateway and Document Management System Privacy Impact Assessment for privacy-related factors, which is published at www.dhs.gov/privacy.

suspected of posing a threat to aviation security. Like the Registered Traveler program, TSA seeks to add a layer of protection to the KT applicant by providing this further review of potential matches between his or her information and information within the threat assessment databases. After TSA review, the name of any passenger considered to be posing or suspected of posing a threat to aviation security will be forwarded to appropriate law enforcement and/or intelligence agency(ies) for either action or further investigation. Such an individual will not be approved as a Known Traveler and his or her card will not be activated. KT applicants' biographical and biometric information will be maintained in the TSA system whether or not their KT card is activated.

TSA will transmit in an encrypted fashion to the Private Sector Partner the names of those volunteers who have cleared the security threat assessment. The Private Sector Partner will encrypt the data about Known 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 Private Sector Partner, will send an e-mail to the KT applicant, via the e-mail account provided at enrollment, or via other appropriate means, informing the traveler of his/her status in the program (either accepted or rejected). All volunteers may inquire whether they have been granted KT status by calling a hotline or accessing a website established by the Private Sector Partner.

B) Use of KT Privileges

PSKT airports will have a kiosk staffed by the Private Sector Partner and located before the TSA screening checkpoint at an airport. A Known Traveler will approach the kiosk staffer, present his or her card, and then insert the card into the kiosk. The Known Traveler will submit his or her biometrics at the kiosk. The system will match the participant's biometric information to the biometric information stored on the card for identity verification. If the match fails, the system will prompt the person to try again or to switch to the secondary biometric (e.g, the iris if the fingerprint is the primary biometric and vice versa). After a set number of failed attempts, the individual will not be allowed to access the PSKT lane. Upon verifying the person's identity, the system will then check his or her status with the program.[5] A positive check will allow verified participants to proceed through the KT security checkpoint. Any participant whose biometric cannot be matched or eligibility verified will be directed to the regular security checkpoint lines.

This pilot program will not supplant regular screening procedures, unless identified by TSA, during the screening process. Known Travelers remain subject to routine passenger screening at airport security checkpoints (e.g., walk through metal detectors).

[5] In all cases, names will be periodically run against the terrorist and criminal databases throughout the course of the program in order to ensure that all enrollees remain eligible. TSA may deactivate a Known Traveler's or Register Traveler's privileges based on a changed result in the threat assessment.

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

Because PSKT is a strictly voluntary program, consent is a prerequisite for participation in the program. During the PSKT pilot, the Private Sector Partner will provide a notice required by the Privacy Act, 5 U.S.C. 552a(e)(3), to volunteers regarding the information collected in order for TSA to conduct security threat assessments. 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 by TSA. Additionally, the Private Sector Partner will provide KT applicants with a copy of its written privacy policy. Individuals who choose not to apply or participate in the program will not be penalized and can continue to fly commercially by undergoing normal airport security screening procedures.

The collection, maintenance, and disclosure of information collected for TSA to conduct a security threat assessment will be in compliance with the Privacy Act and the published system of records notice for RT pilots, DHS/TSA 015. In conducting security threat assessments, information about KT applicants will be shared with TSA employees and contractors who have a "need to know" for implementing the PSKT pilot. 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.

TSA will not disclose the details of the security threat assessment to the Private Sector Partner or its agents. However, TSA will provide the Private Sector Partner with the positive or negative results of the threat assessment so that the Private Sector Partner may notify KT applicants of their enrollment status and provide approved participants with KT media.

As stated earlier, if TSA determines during the threat assessment that a KT applicant may pose or is suspected of posing a threat to aviation security, TSA will notify the appropriate law enforcement and/or intelligence agencies.

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

No. PSKT is a sub-pilot of the Registered Traveler program and operates under the existing Registered Traveler (RT) Operations Files system of records. That system of records notice (DHS/TSA 15) 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 by the Private Sector Partner will be used by TSA to establish a KT and verify a participant's identity. The biographical information will be used to conduct a security threat assessment by means of queries against terrorist and government databases. The Private Sector Partner will not collect biographic or biometric information from KT applicants to use for purposes other than conducting PSKT without the express permission of the volunteer.

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

Information that is requested by TSA to be 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 PSKT pilot; 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.

If the Private Sector Partner seeks to collect any information beyond what is required by TSA, it must inform the applicant or participant that the information is not required by TSA. The applicant or participant, at his or her discretion, may supply additional information requested by the Private Sector Partner or any other information that he or she chooses to provide.

How will the information be secured against unauthorized use?

TSA will secure personal information against unauthorized access and use through a defense in-depth cyber security strategy. Layered IT security architecture will protect data from the time it is collected, through transmission and into storage. TSA will utilize known IT security practices and polices, and will utilize the National Institute of Standards and Technology (NIST) risk management methodology. Data will be categorized using FIPS Publication 199 and security controls applied accordingly. In addition, TSA will adhere to the Department of Homeland Security Acquisition Regulation (HSAR) standards which address personnel security standards for contractors. All critical system data will undergo stringent review and assessment process conducted by the IT security offices on an annual as well as ad hoc basis.

TSA will follow all mandatory federal regulations which will include, but not be limited to: the Privacy Act of 1974, as amended (5 USC 552a), which affords individuals the privacy protection in records that are maintained and used by Federal agencies, the Federal Information Security Management Act of 2002, (Public Law 107-347), which establishes best security practices and security performance metrics for Federal IT 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.

How will the KT 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 KT status. Because this program is in the pilot phase of operations, KT applicants 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 KT Pilot become a fully operational program as part of the Registered Traveler Program, TSA will develop redress procedures for individuals who seek to participate in the program.

In the interim, individuals may contact the TSA Ombudsman, an independent office dedicated to assisting the public and TSA employees resolve any question or concerns they may have with TSA in a confidential and impartial manner. As a designated neutral, the Ombudsman does not take sides in a conflict or dispute or advocate for any individual or party. Though a member of the Ombudsman staff may sometimes contact others on an individual's behalf – and with the individual's permission – the Ombudsman does not have the power or authority to impose resolutions or binding decisions.

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 at the PSKT pilot site by the Private Sector Partner.
- The Private Sector Partner will encrypt the data and forward it to TSA, TSA's agent or the TSA Clearinghouse and then send it to the Gateway.
- TSA will conduct the security threat assessment by running the names against terrorist related and appropriate government databases.
- The results of the checks are reviewed by the appropriate 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 threat to aviation security will not be activated into the program, 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 Private Sector Partner, TSA will adhere to the Department of Homeland Security Acquisition Regulation (HSAR) standards which address personnel security standards for contractors who will load the information on their workstations at the respective PSKT site to activate the credentials of eligible enrollees.
- Each time a Known Traveler offers his or her KT card at a PSKT 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?

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 or on other approved media 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. Moreover, the system complies with NIST standards and Federal statutory requirements for privacy and security.

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. TSA will adhere to the HSAR standards which address personnel security standards for contractors.

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

All Private Sector Partners and their contractors are also required to have the appropriate training and clearances relevant to their duties.

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

Appendix A

PSKT Airport	Private Sector Partner
Orlando International Airport (MCO)	Greater Orlando Aviation Authority (GOAA)