Privacy Impact Assessment
for the

Registered Traveler Pilot (Private Sector Subpilot)

September 20, 2005

Contact Point
Lisa S. Dean
Privacy Officer
Transportation Security Administration
(571) 227-3947

Reviewing Official
Nuala O'Connor Kelly
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

1. 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 the 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 technologies for biometric identification 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 undergo a security threat assessment. The security threat assessment includes running the volunteers' biographical information through terrorist-related databases, criminal databases for outstanding warrants, and other government databases that TSA maintains or uses in order to confirm that volunteers are U.S. citizens, lawful permanent resident aliens or nationals of the United States, and to ensure that the volunteer does not pose or is not suspected of posing a threat to transportation security. If RT volunteers pass the security threat assessment, their membership in RT is activated. RT Volunteers then have the option of using their RT benefits when traveling at participating RT airports. As part of the RT operations, TSA uses participants' biometric information to verify their identity and membership status when they present themselves for screening at the airport security checkpoint. These procedures should expedite the screening of Registered Travelers and allow TSA to focus its security efforts on passengers who have not undergone security threat assessments and may pose a risk to aviation security.

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 resulting in an impact to personal privacy.

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 SORN for RT pilots, DHS/TSA 015, and the SORN for the Transportation Security Threat Assessment System, DHS/TSA 002. In conducting security threat assessments, information about KT applicants will be shared with Department of Homeland Security (DHS) employees and contractors who have a "need to know" for implementing, monitoring, and evaluating the PSKT sub-pilot. The SORNs reflect the appropriate routine uses for disclosure of this information to the TSA contractors. The TSA contractors are contractually obligated to comply with the Privacy Act in their handling, use, and dissemination of personal information. TSA may also share information with DHS officials and employees that need the information for the performance of official duties. For example, information may be shared with ICE for review of immigration status. If persons pose or are suspected of posing a security threat, then TSA will notify the appropriate law enforcement and/or intelligence agency.

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 and for DHS/TSA 002. Specifically, the information will be used by and disclosed to DHS

personnel and DHS contractors or other agents who need the information to conduct security threat assessments and to assist in the maintenance and monitoring of the operation of the PSKT pilot. TSA may also share information with DHS employees and officials who need the information for the performance of official duties. For example, information may be shared with ICE for review of immigration status. If persons pose or are suspected of posing a security threat, then TSA will notify the appropriate law enforcement and/or intelligence agency.

This Privacy Impact Assessment (PIA) is the second amendment of the PIA published by TSA on June 24, 2004. TSA has revised the security threat assessment required for individuals who participate in the Private Sector Known Traveler (PSKT) sub-pilot to include an immigration status check. In order to be eligible to participate in PSKT, individuals must be U.S. citizens, U.S. nationals, or lawful permanent resident aliens. Immigration status information will be verified during the TSA security threat assessments in order to confirm participants' eligibility for this program and to identify individuals who may otherwise pose or be suspected of posing a threat to transportation security.

Because of the success of the Registered Traveler Pilot Program, TSA is 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 launched a sub-pilot program known as PSKT.

This revised Privacy Impact Assessment (PIA) for the PSKT sub-pilot is published in accordance with the requirements of the E-Government Act of 2002 (P.L. No. 107-347). TSA has entered into an agreement to conduct a PSKT subpilot which will revise TSA's role by incorporating a Private Sector Partner that will carry out certain responsibilities. 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 as RT, 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 results to the volunteer's biometric information; and 4) verifying the identity of an enrollee prior to 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 security threat assessment and periodic reassessments, which includes confirmation of volunteers' status as U.S. citizens, lawful permanent resident aliens, or nationals of the United States; providing standards for the Private Sector Partner's operations; conducting security threat assessment screening; and oversight. To leverage the business processes of the private sector, the Private Sector Partner will have responsibility for procurement, marketing and operational functions (including identity verification using biometric data), consistent with TSA guidelines and Federal technology standards for Information Technology and biometric security.

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.

The Private Sector Partner collects the KT applicant's pertinent biographic and biometric information and sends it to TSA to conduct security threat assessments. These assessments include running

the applicant's biographical information through Federal databases, including the Terrorist Screening Data Base (TSDB) and the TSA selectee list, against databases containing outstanding wants and warrants, and against other governmental sources maintained or used by TSA to ensure that KT applicants are U.S. citizens, lawful permanent resident aliens or nationals of the United States and do not pose or are not suspected of posing a threat to aviation security. All pilot participants (Registered Travelers and Known Travelers) undergo the same security threat assessments. Once TSA completes the initial security threat assessment, the agency will inform the Private Sector Partner whether the KT applicant has been approved or not approved.1 However, the details of the security threat assessments will be retained by TSA and not shared with the Private Sector Partner or KT applicant. The Private Sector Partner will inform the individual KT applicant whether he or she has or has not been accepted.

2. Definitions

Approved Security Threat Assessment – means TSA's determination that an individual has been approved to participate in RT, including the PSKT sub-pilot.

Biometric Data – means data or information derived from technology that measures and analyzes physiological or behavioral characteristics that can be verified technologically. In this PIA, it specifically refers to data in the form of images and/or templates regarding the fingerprints and irises of an RT (or PSKT) applicant or participant.

Enrollment – means the process by which a KT applicant's biographical and biometric information is captured.

Gateway Infrastructure – means the TSA information technology system that interfaces among security threat assessment databases, adjudication center, and the Private Sector Partner.

KT Applicant – means a volunteer who chooses to participate in PSKT and whose initial security threat assessment is pending.

KT card – means the token issued by the Private Sector Partner to Known Travelers to enable them to access KT benefits upon acceptance into the program. It includes an Integrated Circuit Chip (ICC) containing encrypted select biometric data necessary for program operations.

Known Traveler (KT) – means a volunteer traveler who has received an Approved Security Threat Assessment and who is participating in the Private Sector Known Traveler Program.

Lawful permanent resident – means an individual who has been lawfully admitted to the United States for permanent residence, as defined in 8 U.S.C. 1101.

National of the United States – as defined in 8 U.S.C. 1101, means a citizen of the United States or a person who, though not a citizen of the United States, owes permanent allegiance to the United States.

Not Approved Security Threat Assessment – means TSA's determination that an individual is not authorized to participate in Registered Traveler Pilot Program or the PSKT sub-pilot due to the results of the security threat assessment.

1 TSA conducts ongoing security threat assessments, and, as a result of the latest information, the approval status of any KT participant may change.

Private Sector Known Traveler (PSKT) – means the Registered Traveler Pilot Program sub-pilot applying a Federal Government – Private Sector partnership to the Registered Traveler concept.

Private Sector Partner – means the private sector entity that has entered into an agreement with TSA to undertake specific responsibilities for PSKT at a specific airport(s), as well as its agents and contractors (unless otherwise specified).

Registered Traveler (RT) – means a volunteer who chooses to participate at one of the RT Pilot Program airports, passed his or her threat assessment, and is currently eligible for RT privileges.

Registered Traveler Pilot Program – means, activities undertaken under the authority provided in the Aviation and Transportation Security Act (ATSA) (P.L. 107-71) Section 109(a)(3). It includes, but is not limited to RT-related activities at the following airports: Minneapolis-St. Paul (MSP), Los Angeles International (LAX), George Bush Houston Intercontinental (IAH), Boston Logan (BOS), and Washington Reagan National (DCA) airports.

Security Threat Assessment – means the TSA's check of an applicant's information against the terrorist watchlists drawn from the Terrorist Screening Database (TSDB) maintained by the Terrorist Screening Center, against databases containing outstanding wants and warrants, and against other governmental sources to confirm that volunteers are U.S. citizens, permanent resident aliens or U.S. nationals in order to determine an applicant's eligibility for participation in RT, including the PSKT sub-pilot.

TSA – means the Transportation Security Administration, the Department of Homeland Security, or any successor Federal Government entity.

Vetting Platform – means the Information Technology systems used to conduct the Security Threat Assessments and interface with the TSA Gateway Infrastructure.

3. System Overview

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

The Private Sector Partner will collect the information from KT applicants needed for TSA to conduct the security threat assessment. KT applicants volunteer to provide their biographic and biometric information to use for security threat assessments and identity verification purposes, respectively.

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 be asked to provide the following biographic information: full name (first, middle (if applicable) and last names(s)), social security number2 or alien registration information (if

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

applicable), other names used, home address, home telephone number, cell phone number, e-mail address, date of birth, place of birth, nationality, gender, prior addresses (for the past five years), driver's license number, and physical description.3 Biometric identifiers to be collected include images of all available fingerprints and photographs of both irises (if available).4 E-mail information is used to contact KT applicants concerning their enrollment status or major changes to the program.5 TSA will run this information through Federal databases, including the TSDB and the TSA selectee list, and other governmental databases it maintains or uses to complete a name-based security threat assessment, which includes verification of immigration status to ensure that volunteers are U.S. citizens, lawful permanent resident aliens or nationals of the United States prior to acceptance of the KT applicant as a Known Traveler participant in this pilot program,

3.2 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, which is linked to their biometric information, if they are accepted. As explained above, TSA requires that the Private Sector Partner use biometric data to verify the identity of Known Travelers at the verification kiosk prior to the designated 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 through TSA-conducted security threat assessments;
2. To expedite security screening at airport checkpoints for accepted Known Travelers whose identities are verified by using biometrics at verification kiosks;
3. To assist in the management of the records of KT applicants and current KT participants;
4. To permit the retrieval and updates of the results of ongoing TSA security threat assessments performed on volunteers;
5. To refer to the appropriate intelligence and law enforcement entities the identity of KT applicants, based on ongoing security threat assessments, who pose or are suspected of posing a threat to aviation security; and
6. To conduct metrics analysis of the pilot operations, which will assist TSA and DHS in structuring any necessary modifications to the program.

3 Physical description information means height and eye color.

4 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.

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

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

3.3.1 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 and smart card technologies used in this pilot meet all applicable National Institute of Standards and Technology, American National Standards Institute, Federal Information Processing Standards and Government Smart Card standards.

Documents provided by the enrollee for personal identity verification will be scanned and authenticated by the Private Sector Partner and maintained in accordance with the requirements of the Privacy Act of 1974 and the Private Sector Partner's Privacy and Fair Information Practices and policies. The applicant's enrollment information will be stored by the Private Sector Partner.

Once the enrollment is completed, the Private Sector Partner may choose to issue an inactive KT card to the applicant with a template of his or her biometrics encrypted and encoded on it. If the candidate receives the KT card in advance of passing the security threat assessment and being accepted into the program, the KT 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 the candidate is not suspected of posing a threat to aviation security. If the Private Sector Partner chooses to issue the KT card after the threat assessment is complete and the candidate is accepted into the program, the Private Sector Partner may deliver the KT card by mail, by pick up in person by the KT applicant, 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 (SORN) for the RT Pilot (DHS/TSA 015) and for the Transportation Security Threat Assessment System (DHS/TSA 002). All biometric data will be stored on the Private Sector Partner's database and will be secured and maintained in a secure/locked location by their agent (contractor) for the duration of their contract. In addition, select biometric data, necessary for operations, will be encrypted and stored on the KT Integrated Circuit Chip (ICC) contained on the KT cards. During enrollment, the KT applicant's information will be securely stored and encrypted 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 KT card and in the PSKT/Registered Traveler database at the pilot location and at TSA or TSA's designated agent.

All biometric information collected will be used for enrollment in the program and to verify identification at the verification kiosk prior to the designated security checkpoint. Biometrics will not be used to conduct security threat assessments during the pilot phase of the program.

The biographical information will be used by TSA to conduct a security threat assessment by running the names and biographic information through Federal databases, including the TSDB and the TSA selectee list, appropriate criminal databases, and through other government databases that TSA maintains or uses to verify that KT volunteers are U.S. citizens, lawful permanent resident aliens or nationals of the United States and do not pose or are not suspected of posing a threat to transportation security. The end

result will be the person receiving either an Approved Security Threat Assessment or a Not Approved Security Threat Assessment. In conducting the security threat assessment, TSA will store and distribute information to the TSA vetting platforms and TSA adjudication center using the Gateway Infrastructure maintained by the TSA Office of Transportation Vetting and Credentialing (OTVC).6

During the security threat assessment process, 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 suspected of posing a threat to aviation security. As with other pilots in 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 volunteer 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). Such an individual will receive a Not Approved Security Threat Assessment, will not be approved as a Known Traveler, and his or her KT card will not be activated. KT applicants' biographical and biometric information will be maintained in the TSA system whether or not they are accepted into the program.

Upon completion of its security threat assessment analysis, TSA will transmit in an encrypted fashion to the Private Sector Partner (but not its agents) the names of those volunteers who have been approved or not approved. TSA will only transmit the name of the individual and the individual's status (approved or not approved). The Private Sector Partner or its agent will then notify the KT applicant, via the e-mail account provided at enrollment, or via other appropriate means, of his/her status in the program (either approved or not approved).

All volunteers may also inquire whether they have been granted KT status by calling a hotline or accessing a website established by the Private Sector Partner.

The Private Sector Partner will encrypt the received data about the approved Known Travelers onto removable media and transfer the data, in a secure fashion, to their secure desktop/laptop computers at the airport enrollment and verification kiosks stations near the designated security checkpoints.

TSA conducts ongoing security threat reassessments and, as a result of the latest available information, the status of approved Known Travelers is subject to change. Should the status of any approved Known Traveler change to a "not approved" status, TSA will notify the Private Sector Partner, which in turn will notify the individual and deactivate the individual's KT card. Revocation of status by TSA will be made for security reasons and not for any financial reasons based upon fee requirements stipulated by the Private Sector Partner. The Private Sector Partner on its own authority may revoke a KT's status as an active member for reasons regarding the fee requirement.

3.3.2 Use of KT Privileges

PSKT airports will have a verification kiosk staffed by the Private Sector Partner and located before the TSA screening checkpoint at an airport. A Known Traveler will approach the verification kiosk staffer, present his or her KT card, and then insert that card into the verification kiosk. The Known Traveler will submit his or her biometrics at the verification kiosk. The system will match the participant's biometric

6 See OTVC Screening Gateway and Document Management System Privacy Impact Assessment for privacy-related factors: this document is published at www.dhs.gov/privacy.

information to the biometric information stored on the KT 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.7 A confirmation that a person's status is active 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.

All Known Travelers and Registered Travelers must go through the normal screening process at airport security checkpoints (e.g. walk through metal detectors); however, they are not subject to additional screening, unless warranted.

3.3.3 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 and, if applicable, the written privacy policy of the Private Sector Partner's agents. 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.

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 result (approved or not approved) of the security threat assessment so that the Private Sector Partner or its agent will notify KT applicants of their enrollment status and provide approved participants with KT credentials.

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.

3.3.4 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 015) was published in the Federal Register on June 1, 2004 and can be found at 69 Fed Reg. 30948, 30950. PSKT, as a sub-pilot of RT, also is included under the Transportation Security Threat Assessment System (T-STAS) systems of record notice (DHS/TSA 002) published in the Federal Register on September 24, 2004, and amended on December 10, 2004. It can be found at 69 Fed. Reg. 57348, 57359; and at 69 Fed. Reg. 71837.

7 In all cases, names will be run, on an ongoing basis, against terrorist, criminal and other applicable government databases throughout the course of the pilot to ensure that each enrollee remains eligible. TSA may deactivate a Known Traveler's or Registered Traveler's privileges based on a changed result in the security threat assessment indicating that the individual poses or is suspected of posing a threat to aviation security.

3.3.5 What is the intended use of the information collected?

The biographical information will be used by TSA to conduct a security threat assessment by means of checks against government databases. The biometric information being collected by the Private Sector Partner will be used to establish and verify an approved KT applicant's identity. The Private Sector Partner will not collect biographic or biometric information from KT applicants for purposes other than conducting PSKT without the express permission of the applicant.

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

If the Private Sector Partner seeks to collect any information beyond what is required by TSA, it must inform the applicant or participant that said additional 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. Failure to provide such additional information will not affect the eligibility for the KT program.

3.3.7 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, and 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.

3.3.8 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.

3.3.9 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, and those current KTs whose status changes as a result of ongoing security threat assessments analysis will have their KT status revoked. 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.

3.3.10 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 biographic information will be collected from a form available on the Private Sector Partner's website, from a form at the Private Sector Partner's enrollment station, or by manually entering the information, supplied by the individuals enrolling in the pilot program at the PSKT pilot site, into a computer. All biometric information must be submitted by the individuals physically present at the PSKT enrollment station. All of these activities will be performed by the Private Sector Partner.

- The Private Sector Partner will encrypt the biographic data and forward it to TSA, TSA's agent or the TSA Clearinghouse and/or then send it to the Gateway.

- TSA will conduct the security threat assessment by running the names against Federal databases that TSA maintains or uses.

- The results of the checks are reviewed by the appropriate TSA personnel or TSA's agents for accuracy. TSA will further vet persons identified as potential matches against additional databases to further determine accuracy. Any individuals who TSA determines pose or are suspected of posing a threat to aviation security will not be accepted into the program. Also, individuals who do not meet the eligibility criteria, such as those who are not U.S. citizens, lawful permanent resident aliens or nationals of the US, will not be accepted into the program. For those KT applicants whose status changes as a result of ongoing security threat assessments, TSA will revoke their KT status, as warranted.8 TSA will disclose that individual's biographic and/or biometric information to the appropriate law enforcement and/or intelligence agencies if the individual poses or is suspected of posing a security threat.

- The results of the security threat assessments (whether the applicant is approved or not) are encrypted and sent back to the Private Sector Partner. The Private Sector Partner or its agent will then notify KT applicants of their enrollment status and supply approved KT applicants with an activated KT credential. TSA and its Private Sector Partner 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 sites.

8 KT or RT status may also be revoked by TSA for abuse of the rules governing the security benefits accorded Known and Registered Travelers.

- Each time a Known Traveler offers his or her KT card at a PSKT pilot verification kiosk location, the identity of the volunteer is authenticated by verifying that the biometric on the KT card matches the individual's biometric at the verification kiosk, placed prior to the designated screening checkpoint.
- In addition, after biometric verification of an individual's identity, their status in the system is determined. This process will also indicate whether the individual remains eligible from a security standpoint. If not, the individual's KT card will be deactivated.
- A KT participant whose status is currently approved is then either afforded access to the PSKT lane or directed towards the front of a regular screening lane.

3.3.11 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 TSA 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 contractors also hold 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:

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, 571-227-3813

Appendix A

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