Privacy Impact Assessment
for the

TSA Traveler Identity Verification Program

August 31, 2006

Contact Point
James Kennedy
Director, Office of Transportation Security Redress
Transportation Security Administration
TSARedress@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
Privacy@dhs.gov

Abstract

The TSA Traveler Identity Verification Program was developed as a voluntary program by the Transportation Security Administration (TSA) to provide a forum for individuals who believe they have been unfairly or incorrectly delayed, denied boarding, or identified for additional screening at our Nation's airports to request redress. Responsibility for the program lies in TSA's Office of Transportation Security Redress (OTSR). TSA will review the submission and reach a determination of whether its watch list clearance process may aid in expediting a passenger's check-in process for a boarding pass. TSA will use this information to attempt to help those individuals who have been delayed or prevented from traveling as a result of TSA's airport security measures. TSA will transmit the Cleared portion of the Federal Watch List to airlines to assist them in distinguishing and clearing individuals who initially presented as matches. OTSR will share information provided by individuals seeking redress with the TSC and nominating law enforcement and intelligence agencies to determine if the individual is a positive match to the watch list.

Introduction

TSA has broad authority under 49 U.S.C. § 114(f) to assess threats and threat information related to transportation and to plan and take appropriate action to address threats to transportation. Historically, nine government agencies maintained 12 different watch lists intended to accomplish a variety of goals. Two of those lists included the No-Fly List and the Selectee List. The No-Fly List is a list of individuals who are prohibited from boarding an aircraft. The Selectee list is a list of individuals who must undergo additional security screening before being permitted to board an aircraft.

The No-fly and Selectee Lists were maintained by the TSA when it was a component of the Department of Transportation and later became a component of the Department of Homeland Security (DHS). More recently, in accordance with Homeland Security Presidential Directive 6, issued on September 16, 2003, the No-Fly List and a portion of the Selectee List were consolidated within the Terrorist Screening Database (TSDB), maintained by the Terrorist Screening Center (TSC). The TSC was established to consolidate the government's approach to terrorism screening and to provide for the appropriate and lawful use of terrorist information in screening processes. The TSC maintains responsibility over the Federal Government's consolidated terrorist watch lists, including the No-Fly and a portion of the Selectee Lists in the TSDB. TSA maintains a portion of the Selectee List that includes individuals who pose a threat to transportation security who may not have links to terrorism. The No-Fly and Selectee List components of the TSDB and the portion of the Selectee List maintained by TSA are collectively referred to as the "watch list."

OTSR was created to provide a forum for individuals who have been identified either correctly or incorrectly as a threat to transportation security to appeal that determination and petition to have erroneous information corrected. OTSR serves as a single point of contact for individuals and organizations interested in the Traveler Identity Verification Program, and

provides coordination and support for redress requests for transportation security programs. OTSR will share information provided by individuals seeking redress with the TSC and nominating law enforcement and intelligence agencies to determine if the individual is a positive match to the watch list.

A Traveler Identity Verification Form (TIVF) is used for collecting personal information for the Traveler Identity Verification Program. Appendix A contains a copy of this form. OTSR created the Redress Management System (RMS), which is the information technology system that maintains information concerning the status of redress requests. Information contained in RMS includes the information collected from individuals in support of their redress requests (on the TIV Form), the current status of redress requests received, and redress related correspondence between TSA and the requestor. The RMS will also maintain information about applicants seeking redress for programs in which they have applied for a right, benefit, or privilege and were denied by a transportation security credentialing program.

Section 1.0
Information collected and maintained

1.1 What information is to be collected?

The information collected from individuals applying to the Traveler Identity Verification Program consists of full name, current address, date of birth, gender, place of birth, Social Security Number, height, weight, hair color, eye color, and home and work telephone numbers. The individual may submit to TSA either a copy of a U.S. Passport or copies of at least three of the following: a birth certificate, driver's license, immigrant/nonimmigrant visa, naturalization certificate, certificate of citizenship, voter registration card, certificate of release or discharge from active duty, government identification card or military identification card. If the passenger submits a birth certificate, it must be a certified copy of the original. In the future, TSA also is planning to request the individual to provide the name of the airline, flight number, and date that he/she was either delayed or denied boarding. Appended to the TIVF, is a Privacy Act statement and an acknowledgment that the information the individual provides is true and correct and that he or she is providing the personal information voluntarily. The individual must sign and date the acknowledgement under the penalty of perjury. The results of the matching against the Federal watch list will be captured and maintained in a data field in the Redress Management System.

1.2 From whom is information collected?

TSA will collect information directly from the individual applying to the Traveler Identity Verification Program who believes that he or she has been negatively affected by watch list clearance procedures conducted by the airlines who are required to use the Federal watch list and its implanting security directives.

1.3 Why is the information being collected?

The information is being collected in order to conduct redress for individuals who believe that they have been unfairly or incorrectly delayed, denied boarding, or identified for additional screening at our Nation's airports. The flight information will assist TSA in coordinating with the airline.

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

TSA has broad authority under 49 U.S.C. § 114(f) to assess threats and threat information related to transportation and to plan and execute such actions as may be appropriate to address threats to transportation. The Privacy Act of 1974 provides additional authority for an individual redress program. The TIVF, available on TSA's website at www.tsa.gov and provided in Appendix A, defines the collection of personal information for the Traveler Identification Program.

1.5 Privacy Impact Analysis

TSA will collect the names and personally-identifying information of individuals who believe they have been unfairly or incorrectly delayed, denied boarding, or identified for additional screening at our Nation's airports, and who voluntarily submit their information. While the information collection is fairly broad, it is limited to information used to identify the individual and possibly distinguish the individual from someone with a name similarity, and has been designed to accomplish that goal. OTSR has developed a secure web-based application intake portal that will enable the passenger to submit his/her request for redress. TSA will maintain this data in a secure system consistent with the requirements of the Privacy Act.

Section 2.0
Uses of the system and the information

2.1 Describe all the uses of information.

TSA will use the personal information to provide the individual redress. If an individual has been mistaken for an individual who is actually on the watch lists, TSA will use the additional information collected from the individual to verify his/her identity as distinct from persons who are in fact on the watch list. Airlines have secure access to the web board TSA list for clearing individuals who may initially present as matches to the Federal watch list. Airline personnel can then complete the passenger check-in process more quickly while implementing TSA-required identity verification procedures. The watch list is Sensitive Security Information (SSI) that must be handled in accordance with 49 C.F.R. Part 1520. In the event that the individual is a positive or suspected match to the TSDB, TSA will review the information and work with the Terrorist Screening Center to update information that may be contained in the system in compliance with established transportation security procedures.

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.

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

TSA will collect personally identifiable information directly from the individual seeking redress. In addition, TSA requires the passenger to submit proof of identity consisting of photocopies of a U.S. Passport or copies of at least three government-approved or issued documents, as described above.

2.4 Privacy Impact Analysis

Since the personal information is collected directly from the individual and he/she is required to acknowledge and attest under the penalty of perjury that the information in the TIVF as well the identity documents are accurate, the risk of collecting inaccurate information is minimized. Uses of the information are for purposes of assisting the individual or ensuring an appropriate response in the event of a match to an individual on a watch list.

Section 3.0 Retention

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

TSA is currently working to develop a schedule to cover the personal information collected from individuals who avail themselves of the redress process. This schedule will provide a retention period, which will also be reflected in a Memorandum of Understanding (MOU) between TSA and TSC. At this time, TSA anticipates that the retention period for these records will be a minimum of 6 years in accordance. This retention will ensure that records are available for litigation purposes. TSA will not destroy these records until a schedule is finalized and approved by NARA.

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

TSA is working to develop a schedule to cover records about individuals utilizing the redress process, which it will submit to NARA for review and approval. Until a retention schedule is submitted and approved by NARA, no data collected for the redress process will be destroyed.

3.3 Privacy Impact Analysis

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. TSA expects that records collected from applicants to the Traveler Identity Verification Program will be kept for a minimum of 6 years. This 6 year retention will ensure that records are retained in the event an individual chooses to sue TSA within the 6 year statute of limitations set forth in 28 U.S.C. § 2401(a).

Section 4.0
Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

In the ordinary course of administering the Redress Program, the information is expected to remain within OTSR. The information TSA receives from individuals may be shared with DHS employees and contractors who have a need for the record in the performance of their duties, including but not limited to law enforcement or intelligence operations. This information will be shared in accordance with the provisions of the Privacy Act, 5 U.S.C. § 552a.

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

TSA may share information submitted by individuals applying to the Traveler Identity Verification Program within DHS as needed for administrative, intelligence, counterintelligence, law enforcement or other official purposes related to transportation or national security in accordance with the provisions of the Privacy Act. TSA may also share the results of the redress effort with these same organizations. For example, information may be shared with legislative staff if an individual contacted their Congressman regarding their experience, or may be shared with intelligence if a positive match to the watch list submits information.

4.3 How is the information transmitted or disclosed?

Depending on the specific situation and need, a designated TSA official may transmit this data in person, paper format, via a secure data network, via facsimile or telephonically within DHS only to those who have a need for the information in the performance of their duties. This method of transmission may vary according to specific circumstances. The program director will grant access to the system to those individuals who have a sustained need to access the information to perform their duties. The program director will determine the level of access required on an individual basis and will restrict the user's account as appropriate.

4.4 Privacy Impact Analysis

Information sharing is limited to DHS employees and contractors who have a need for the record in the performance of their duties in accordance with the Privacy Act. Privacy protections will include strict access controls, (passwords and role-based access), tracking features, and mandated training for all employees and contractors.

Section 5.0
External sharing and disclosure

5.1 With which external organizations is the information shared?

TSA will share information it receives with the Terrorist Screening Center (TSC), airport and airline operators. TSA may share information it receives outside of DHS 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 in accordance with the routine uses identified in the applicable Privacy Act system of records notices (SORNs) DHS/TSA 006, Correspondence and Matters Tracking Records, and DHS/TSA 011, Transportation Security Intelligence Service (TSIS) Operational Files. DHS/TSA 006 was last published in the Federal Register at 68 Fed. Reg. 49,496, 49,503 (August 18, 2003), and DHS/TSA 011 was last published in the Federal Register at 69 Fed. Reg. 71,828, 71,835 (December 10, 2004).

5.2 What information is shared and for what purpose?

TSA will share the name, date of birth, place of birth, gender, passport, driver's license state and number, height, weight, hair color and eye color of individuals whose identities have been verified as distinct from persons who are in fact on the watch list with the airlines so that airline personnel can complete the passenger check-in process for those individuals that have participated in the redress process more quickly while implementing TSA-required identity verification procedures. TSA may also share individually identifying data with the TSC and the agency that nominated the individual for inclusion on the watch lists when there is a potential match to the Federal watch list, and will work to correct any erroneous information that may be contained in the system.

As noted in Section 5.1, TSA may also share in accordance with its routine uses information about individuals posing or suspected of posing a threat to, transportation or national security outside of DHS for intelligence, counterintelligence, law enforcement or other official purposes related to transportation or national security in accordance with the Privacy Act.

5.3 How is the information transmitted or disclosed?

Depending on the specific situation and need, TSA may transmit this data in person, paper format, via a secure data network, via facsimile or telephonically.

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?

No. The Privacy Act System of Records Notices described above provides the necessary allowances for sharing of the information in accordance with the Privacy Act. TSA plans to enter into an MOU with the TSC as part of a government wide redress MOU. The airlines are required to follow TSA directives covering the use of the Federal watch list.

5.5 How is the shared information secured by the recipient?

Any Federal agency receiving this information is required to handle it in accordance with the Privacy Act and their applicable SORNs. Airlines are required to secure information about individuals and limit disclosure to those who have a need for the information for official purposes, including matching individuals against the watch list.

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

None. However, any Federal agency receiving this information is required to handle it in accordance with the Privacy Act and their applicable SORNs.

5.7 Privacy Impact Analysis

TSA will share this information under the applicable provisions of the SORNs and the Privacy Act. TSA will share information only with those entities that have a need to know the information to perform their official duties. TSA will share identifying information so that airports or airline personnel can readily confirm an individual as one who has been cleared through the TSA redress process.

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), the TIVF provides a Privacy Act Statement. In addition, the individual seeking redress must acknowledge that he/she is voluntarily submitting personal information for redress purposes and that the information provided is accurate. The notice specifies that routine uses of the information may include disclosure for law enforcement, intelligence, or security purposes. The individual must sign and date the acknowledgment under the penalty of perjury. The publication of this PIA and the SORNs DHS/TSA 006, Correspondence and Matters Tracking Records, and DHS/TSA 011, Transportation Security Intelligence Service (TSIS) Operational Files, also serve to provide public notice of the collection, use and maintenance of this information. DHS/TSA 006 was last published in the Federal Register at 68 Fed. Reg. 49,496, 49,503 (August 18, 2003), and DHS/TSA 011 was last published in the Federal Register at 69 Fed. Reg. 71,828, 71,835 (December 10, 2004).

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

Yes. This process is voluntary.

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?

Individuals have the right to decline to engage in the process and to provide their information for review. The individual does not have the right to direct particular uses of the information. TSA will limit its use under the Privacy Act and applicable SORNs which are published in the Federal Register and available for review by individuals interested in knowing how TSA will use and disclose their personal information.

6.4 Privacy Impact Analysis

Individuals are provided a Privacy Act Statement and must acknowledge that he/she is providing correct information and providing the information voluntarily prior to submitting the information to TSA. Therefore, proper notice and an opportunity to voluntarily provide information are provided in order to fully serve the privacy interests of the individual.

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 (URL: http://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 (http://www.tsa.gov/public). In addition, individuals may amend their records through the redress process as explained in paragraph 7.2 below.

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 or may 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 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 passenger submit the completed TIVF to TSA at Transportation Security Administration, TSA-901, 601 South 12th Street, Arlington, VA 22202. This information may help TSA expedite the person's check-in process for a boarding pass. Only the person seeking expedited watch list clearance procedures may submit the TIVF. For those passengers using the web-based application and completing the TIVF online, they may send the documents the documents via hard copy, e-mail or facsimile. For minors, only a custodial parent or guardian may submit the information on behalf of the minor.

- TSA will review the submission and reach a determination of whether its watch list clearance processes may aid in expediting a passenger's check-in process for a boarding pass.

- If the clearance procedures will aid in expediting the person's check-in process, TSA will contact the appropriate parties, such as the airlines, to help streamline the identity-verification process for the individual. TSA will send a letter to the individual to notify them of the completion of the process and advise that the notification letter constitutes a final agency determination that is reviewable by a United States Court of Appeals under 49 U.S.C. §46110.

- While TSA cannot ensure that these clearance procedures will relieve all delays, the procedures should facilitate a more efficient check-in process.

- Passengers who have received TSA's written notification should be aware that clearance at the check-in counter is ultimately based on information that TSA provides to the airlines, not the notification letter.

- If a passenger continues to encounter delays in obtaining a boarding pass at the check-in counter, please contact TSA at the phone number and e-mail listed above.

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

Individuals are notified of the watch list clearance procedures by accessing the TSA public website at the web address listed above, or by contacting TSA at the phone number or e-mail listed above. The airlines also hand out a two-page letter advising the traveler to contact TSA.

7.4 If no redress is provided, are alternatives are available?

Individuals who are unsatisfied with the results of the Traveler Identity Verification Program may appeal the final agency decision to a United States Court of Appeals under 49 U.S.C. § 46110.

7.5 Privacy Impact Analysis

TSA has provided a redress process that furthers the privacy interest of the individual by allowing the individual to be correctly identified. Since TSA will collect information directly from the individual, the risk of collecting inaccurate information is minimized. In addition, individuals may request access to or correction of their personal information pursuant to the Privacy Act.

Section 8.0
Technical Access and Security

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

In order to perform their duties in managing, upgrading, and using the Redress Management System, system administrators, security administrators, IT specialists, redress analysts, intelligence analysts, call center employees, and any other TSA employees with a need for the information to perform their duties may have access to the system. Automated role-based access controls are employed to limit the access of information by different users based on the need to know. The Redress Management System is used internally within TSA for data collection and reporting purposes. No unauthorized users are permitted access to system resources. Strict adherence to access control policies is automatically enforced by the system in coordination with and through oversight by the system administrator.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Contractors who are hired to perform many of the IT maintenance and security monitoring tasks have access to the Redress Management System in order to perform their official duties. Strict adherence to access control policies is automatically enforced by the system in coordination with and through oversight by the system administrator. All contractors performing this work are subjected to Homeland Security Acquisition Regulation (HSAR) requirements for suitability and a background investigation (see 48 CFR 3037.110-70(a)). According to the HSAR, the contractor company is not subject to a clearance process when contracted to work on non-classified awarded contracts or systems, such as RMS. However, all contractor personnel are required to be favorably investigated and adjudicated for suitability before they may be permitted to work on the RMS.

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 system using the policy of Least Privilege, which states that the 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 Redress Management System is secured against unauthorized use 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 system is housed, issued picture badges with integrated proximity devices imbedded, and given specific access to areas necessary to perform their job function. All personnel working/accessing the 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.

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 system based on their function. The system administrator will grant access on a need to know basis. The Facility Security Officer ensures compliance to policy and manages the activation or deactivation of accounts and privileges as required or when expired. TSA ensures personnel accessing the Redress Management 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.

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

The Redress Management System has an audit trail feature to track any changes to the data and to track access to the system. The system has the capability to track individual record access and modifications by user name as well as time/date stamp. The system administrator will regularly review the audit system logs.

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 contractor personnel are required to complete the annual on-line TSA Privacy Training. Compliance with this requirement is audited monthly by the TSA Privacy Office. In addition, security training is provided regularly, which helps to raise the level of awareness for protecting personal information being processed.

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

Information contained in the Redress Management system is safeguarded in accordance with the Federal Information Security Management Act of 2002 (Pub.L.107-347) (FISMA), which establishes government-wide computer security and training standards for all persons associated with the management and operation of Federal computer systems.

The system is currently undergoing a full Certification and Accreditation process and TSA expects to complete this process in August 2006. This process will be completed prior to actual program implementation.

8.9 Privacy Impact Analysis

Data on the system 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 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 trails are maintained and monitored to track user access and unauthorized access attempts.

Section 9.0 Technology

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

The system is primarily built as a modification of Commercial Off the Shelf (COTS) products. System components include modified COTS software, COTS hardware and operating systems.

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

TSA completed a FIPS 199 on May 17, 2006. Security and privacy requirements were derived based on the sensitivity category of the system, which is considered to be Moderate sensitivity. The moderate baseline requirements reflect that stringent controls are needed for protecting the confidentiality, availability, and integrity of data of this system. The system is designed to support the moderate baseline requirements and protects the integrity and privacy of personal information.

The TSA system is designed to allow for collection of only those data elements necessary to allow TSA to complete its 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 distinguish the individual from a person who is on a Federal watch list.

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 not required by the government. 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. Additionally, the record system will track access to electronic information. Access logs will be periodically reviewed. 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.

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.

Conclusion

OTSR provides redress for individuals who believe they have been unfairly or incorrectly delayed, denied boarding, or identified for additional screening at our Nation's airports, through the Traveler Identity Verification Program. TSA is publishing this Privacy Impact Assessment to detail how TSA collects and maintains personal information about individuals who are affected by these redress procedures. Privacy impacts have been mitigated by collecting only information that assists in resolving identification. TSA will use this limited information to help those airline passengers who have been delayed or prevented from traveling as a result of TSA's airport security measures.

Responsible Officials

James Kennedy
Office of Transportation Security Redress
Transportation Security Administration
Arlington, VA 22202

Approval Signature Page

____/s/_____ August 31, 2006

Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration

____/s/_____ August 31, 2006

Hugo Teufel III

Chief Privacy Officer
Department of Homeland Security

Appendix A; Traveler Identity Verification Form

Instructions: Complete all fields. This form may be completed and submitted electronically via www.TSA.gov.

I. Incident Information

Date of	/ /	Airline		Flight No.:	

II. Personal Information

Full Name:	First	Middle	Last

Social Security No.:	- -	Birth Date:	/ / (mm/dd/yy)	Birthplace:	City or Town/Province/Country

Sex:	☐ Male ☐ Female	Height:		Weight:		Hair Color:		Eye Color:	

III. Contact Information

Current Address:	Street Number and Name	Apt. no.

City or Town	State or Province	Zip Code
		-

Home Telephone	( ) -	Work Telephone No.:	( ) -

IV. Required Documentation and Information

You must provide either a copy of a U.S. Passport (Passport No. must be clearly visible) or copies of at least three (3) o the following documents in order for your request to be processed. Check the box next to the document(s) that you ar submitting with this completed form and enter the requested information for each in the space provided.

	Documentation	Information
☐	**U.S. Passport**	Registration No.: Place of issuance:
	OR	
☐	**Birth Certificate**	Registration No.: Place of issuance:
☐	**Certificate of Citizenship**	Certificate No.: Place of issuance:
☐	**Certificate of Release or Discharge from Active Duty (DD Form 214)**	Discharge date: Check one: ☐ Air Force ☐ Army ☐ Marines ☐ Navy ☐ Coast
☐	**Drivers License**	License State of
☐	**Government Identification Card**	Badge No.: Check one: ☐ Federal ☐ State ☐ Local
☐	**Immigrant/Nonimmigrant Visa**	Control no.:
☐	**Military Identification Card**	Card No.: Check one: ☐ Air Force ☐ Army ☐ Marines ☐ Navy ☐ Coast
☐	**Naturalization Certificate**	Certificate State of Country of
☐	**Non U.S. Passport**	Registration Country of
☐	**Voter Registration Card**	Card No.: State of issuance:

V. Nature of Concern (check all that apply)

- ☐ I am unable to print a boarding pass at home or at a kiosk.
- ☐ I missed flight while obtaining a boarding pass.
- ☐ I am directed to a Ticket Counter every time I fly.
- ☐ A Ticket Agent stated that I am on a Watch List.
- ☐ I am not permitted to board a plane.
- ☐ Other _____

_____

_____

VI. Acknowledgement

The information I have provided on this form is true, complete, and correct to the best of my knowledge and is provided in good faith. I understand that knowingly and willfully making any materially false statement, or omission of a materia fact, on this form can be punished by fine or imprisonment or both (see section 1001 of Title 18 United States Code).

I understand the above information and am voluntarily submitting this information to the Transportation Security Administration.

Print or Type Name	Signature	Date

PRIVACY ACT STATEMENT: **Authority:** The authority for collecting this information is 49 U.S.C. § 114. **Principal Purpose(s):** This voluntary submission is provided to afford you the ability to confirm your identity as distinct from an individual on a Federal Watch List. Your Social Security Number (SSN) will be used to verify your identity. Furnishing this information, including your SSN, is voluntary; however, the Transportation Security Administration may not be able to confirm your identity without this information. **Routine Uses:** Routine uses of this information include disclosure to appropriate governmental agencies for law enforcement, intelligence, or security purposes, or to airports or air carriers to verify your identity for purposes of security screening.