Transportation Security Administration

PRIVACY IMPACT ASSESSMENT
FOR
CREW VETTING PROGRAM

July 28, 2004

Point of Contact
Lisa S. Dean
Privacy Officer
Transportation Security Administration

Reviewing Official
Nuala O'Connor Kelly
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 772-9848

PRIVACY IMPACT ASSESSMENT
FOR
CREW VETTING PROGRAM

INTRODUCTION

Program Overview

TSA has been involved in crew "vetting," – the process by which security threat assessments are conducted on airline crewmembers are verified for authenticity – since the program was established by the FAA in October, 2001. On October 19, 2001, the Federal Aviation Administration issued, by way of Emergency Amendment, requirements for submission of cockpit crew lists to ensure vetting through intelligence databases.[1] This EA applied to select foreign countries of concern and required the submission of cockpit crew list information, including crewmember's name, date of birth, place of birth, and pilot/flight engineer license (certificate) number.

In December, 2003, TSA received new information about specific threats to aviation security related to crewmembers on flights to, from, and overflying the U.S. and issued a series of Security Directives (SDs) and Emergency Amendments (EAs) significantly expanding the scope of crew vetting. Requirements specified that applicable air carriers with operations into, out of, and overflying the United States and its territories must submit Master Cockpit Crew Lists which included the cockpit crewmember's name, date of birth, place of birth, and passport number and country of issuance.

On March 30, 2004, TSA issued the most recent SDs and EAs pertaining to crew vetting. These SDs and EAs expanded the definition of "crewmember" from only cockpit crew member to include cabin crew and persons on all-cargo flights. They also expanded the amount of information to be collected to include gender and status onboard aircraft. Persons onboard an all-cargo flight not included in the definition of a crewmember must so indicate their non-crewmember status. In addition all air carriers were required to submit their Master Crew Lists to the U.S. Customs and Border Protection.

Because of the expansion of the definition of crewmember to include cabin crew as well as cockpit crew and persons onboard all-cargo flights, the privacy of a greater number of individuals will be affected by this program. In addition, the transmission of individuals' personally identifiable information originally held by U.S. Customs and Border Protection (CBP) to TSA is a new addition to the program as well as the way in which that information is transmitted from CBP to TSA. Therefore, TSA is conducting this Privacy Impact Assessment to outline how this program will impact the privacy of affected individuals and what steps TSA is taking to minimize that impact. This Privacy Impact Assessment (PIA), conducted pursuant to the E-Government Act of 2002, P.L. 107-347, and the accompanying guidelines issued by the Office of Management and Budget (OMB) on September 26, 2003, is based on the current design of the program and the Privacy Act system of records notice, Transportation Workers Employment Investigations System (DHS/TSA 002), that was published in the Federal Register on August 18, 2003. This PIA provides further details about the collection of personally identifiable information for the purpose of conducting security threat assessments on crewmembers.[2]

[1] Authority to issue Security Directives & Emergency Amendments granted by Aviation & Transportation Security Act (November 19, 2001)

[2] Crewmember is defined as "pilot, copilot, flight engineer, or airline personnel authorized to fly in the cockpit, or cabin crew, as well as any relief or deadheading crewmember.

SYSTEM OVERVIEW

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

TSA will collect and retain personal information about persons authorized to be cockpit and cabin crewmembers on all TSA- regulated passenger and all-cargo flights and non-crewmembers on all-cargo flights. Air carriers and operators are required to provide this information in Master Crew Lists for all crewmembers and non-crewmembers, where appropriate, who potentially will be authorized to be on flights into, out of, or overflying the territorial United States and for all foreign air carrier/operator flights within the territorial United States.

TSA will collect the following information from CBP immediately for the aviation security threat assessment based upon the Master Crew Lists and Flight Crew Manifests: full name (last, first, middle as they appear on the passport or other government issued ID accepted for travel), gender, date of birth[3], passport number and country of issuance[4] and status onboard the aircraft[5]. Additional data to be provided on the master crew list are pilot certificate number and country of issuance (where appropriate). In future phases of this program, TSA will collect a full permanent address and the place of birth for every person contained in a Master Crew List.

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

Based on information from U.S. law enforcement and intelligence agencies, it is necessary for TSA to conduct enhanced security threat assessments for persons authorized to fly in the cockpit or access the cockpit in an operational capacity during flight. By definition this includes all crewmembers as well as all persons onboard all-cargo aircraft operated by any air carrier or operator, foreign or U.S. To assist in the assessment of a crewmember's or non-crewmember's potential threat to aviation security, TSA will collect personal information about them for the purpose of conducting a security threat assessment. This applies to crewmembers on all TSA regulated passenger and all-cargo flights and non-crewmembers for all-cargo flights into, out of, or overflying the territorial United States and for all foreign air carrier/operator flights within the territorial United States. The information will be utilized to mitigate the potential threat from unauthorized persons gaining control of the aircraft while in the territorial airspace of the United States by ensuring that an aviation security threat assessment is performed on persons authorized to be crewmembers or non-crewmembers prior to a flight's operation.

- **What information technology system(s) will be used for this program and how will they be integrated?**

TSA receives individual flight crew manifests[6] from CBP via the secure DHS network and conducts a security threat assessment by running each name on the manifest against law enforcement, immigration, terrorist-related, and intelligence data sources, as well as against the Master Crew List established and maintained by TSA. If all of the required data fields are not included, TSA will request the aircraft operator to supply the missing information.

[3] All individuals who undergo an aviation security threat assessment must submit first name, last name, date of birth, and gender, at a minimum.
[4] TSA and CBP recognize that passport information can only be provided if the individual possesses one. Many countries do not require a passport for immigration purposes and therefore an individual who travels only to such countries may not have obtained a passport since one is not required for travel. TSA also has procedures in place to accept information from those individuals who may have more than one passport.
[5] Status onboard aircraft must be provided during the development of Master Crew List.
[6] Crew manifest is a list of crew members on board on a specific flight.

TSA also collects data from classified and non-classified government and intelligence databases for use in the security threat assessments of crew and non-crewmembers. This information is retained by other U.S. government agencies and is shared with TSA for the purposes of conducting the security threat assessment. The information is updated on a regular basis.

Air carriers submit crewmember information to CBP. This information is transmitted to TSA via the secure DHS network for the purposes of conducting a security threat assessment. All classified material will be handled commensurate with federal guidelines for storing, accessing, sharing, copying, and transmitting classified information. This adds another layer of privacy protection to the crewmember information. TSA will review the results and will make a preliminary determination as to whether a crewmember poses or is suspected of posing a security threat. In the event that TSA makes a negative determination about a crewmember, TSA will notify the air carrier that the crewmember has not been cleared to enter U.S. airspace. TSA will also share information about such crewmembers with the appropriate governmental, law enforcement and intelligence agencies.

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

In accordance with the Aviation and Transportation Security Act of 2001, CBP published an interim rule in the Federal Register on December 31, 2001 (66 FR 67482), as T.D. 02-01, implementing the standards by which passenger air carriers would comply with the requirement to submit crew and passenger manifests for international flights inbound to the United States. The interim rule states that information provided under this rule, upon request, may be shared with other Federal agencies for the purpose of protecting national security.

In its Privacy Act System of Records Notice DHS/TSA 002, TSA provided notice that it is collecting personally-identifying information relating to the Transportation Workers Employment Investigations System. This PIA provides additional notice about the program. TSA intends to provide further notices to individuals in future phases of this program.

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

No. The information collected for the Crew Vetting Program is part of an existing TSA Privacy Act system of records known as the Transportation Workers Employment Investigation System (DHS/TSA 002). The collection, maintenance, and disclosure of information is in compliance with the Privacy Act and the System of Records Notice for DHS/TSA 002, which was published in the Federal Register on August 18, 2003. See 68 Fed. Reg. 49496, 49498. For all-cargo carriers we are covering non-crewmembers (not always air carrier/operator employees but persons whose passage is part of the cargo transportation service) of both U.S. and foreign air carriers/operators, as well as transportation workers who work for foreign air carriers/operators and live/work overseas.

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

TSA will use the information collected to conduct aviation security threat assessments on the covered individuals in the established TSA Master Crew Lists and Flight Crew Manifests. Individuals who are cleared by TSA and/or U.S. law enforcement and intelligence agencies will be added to the Master Crew Lists submitted to TSA or authorized to be a crewmember or non-crewmember, as appropriate, on a Flight Crew Manifest. The Master Crew Lists will be maintained by TSA and will be reviewed on a regular basis to reassess the suitability of those individuals on the list to be authorized crewmembers or non-crewmembers. Flight Crew Manifest submissions will be vetted against the TSA maintained Master Crew Lists to reassess those individuals who have already been authorized through a successfully completed aviation security threat assessment. TSA will also undertake a security threat assessment of covered

individuals submitted on Flight Crew Manifests each time they fly to ensure that any new data that may have become available and affects that individual's authorization is reviewed.

- **With whom will the collected information be shared?**

Personal information for crewmembers and, as applicable, non-crewmembers transmitted via CBP and stored at TSA will be shared only with those U.S. government personnel and contractors with a need to know in order to conduct the aviation security threat assessments. If an aviation security threat assessment reveals that an individual poses or is suspected of posing a security threat, TSA will share that individual's personal information received on Master Crew Lists and Flight Crew Manifests with U.S. law enforcement, to include the FBI and Immigrations and Customs Enforcement (ICE) and intelligence authorities, that supplied the data to confirm the determination. Once a final decision is made by TSA then TSA will notify the appropriate air carriers/operators and, upon its request, the host government.

The collection, maintenance, and disclosure of information about these individuals are in compliance with the Privacy Act and the published system of records notice (DHS/TSA 002).

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

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

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

- Technical limitations on, and tracking of, data access and use;
- Use of secure telecommunications techniques; and
- Limitation of physical access to system databases and workstations.

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

The Privacy Act of 1974, as amended (5 USC 552a), which requires Federal agencies to establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of information protected by the Act.

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

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

TSA is in the process of developing a records retention schedule that will dictate the retention period for these records. Once the records schedule is approved, TSA will amend this document to include the retention period for the crewmember and non-crewmember records. Until the records schedule is approved by the National Archives and Records Administration (NARA), TSA does not have authority to dispose of the records. TSA is proposing that the Flight Crew Manifests will be retained for a relatively

short period of time after completion of the flight and that the Master Crew Lists be retained as necessary for use in the crewmember/non-crewmember aviation security threat assessment process.

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

No. Information is being collected for the purpose of conducting crewmember and, where applicable, non-crewmember aviation security threat assessments in order to protect aviation and national security. As part of this process, information may also be shared with appropriate U.S. government, law enforcement, and intelligence authorities to identify potential threats to transportation security, uphold and enforce the law, and ensure public safety.

- **How will crewmembers and non-crewmembers be able to seek redress?**

In the event that some piece of information is out of date and impacts negatively on the security assessment of an individual, that individual has the ability to seek an adjustment to the adjudication decision and correction of the information through a redress process. The steps outlined below specifically discuss the process for crewmembers and non-crewmembers residing outside the U.S. who believe they have been wrongly identified as a potential threat to aviation security:

1. To request relief, an affected individual may contact the Department of State Consular Section of the nearest U.S. Embassy or Consulate in his/her country of residence. The individual will be asked to provide identifying information as well as sign a statement authorizing TSA to conduct to a background investigation.

2. The U.S. Embassy will securely transmit the information to the Department of State (DOS) Economic Bureau and the appropriate country desk. The appropriate TSA representative will be copied.

3. The DOS Economic Bureau will initiate the redress procedure through TSA. TSA will coordinate the response internally.

4. TSA will coordinate with appropriate U.S. Federal intelligence and law enforcement to determine whether any relief can be provided to the individual.

5. TSA will ask the U.S. Embassy to inform the individual's host government and the individual of TSA's conclusion. In addition, a companion letter will be drafted for the TSA Administrator's signature informing the air carrier of the determination.

6. DOS will send the approved cable to the Embassy and TSA will send the letter via express mail to the airline.

In addition, TSA offers to U.S. based crewmembers and non-crewmembers the opportunity to seek redress by commencing the redress procedure directly with TSA via Office of the Ombudsman.

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

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

- **What is the 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?**

TSA will receive the required crewmember and, where applicable, non-crewmember personal information contained in the Flight Crew Manifest or Master Crew List submitted for the aviation security threat assessment from CBP via the secure DHS network. If all of the required data fields are not included, TSA will ask the aircraft operator to supply the missing information. Master Crew List information must be updated no later than 24 hours prior to a flight on which the crewmember (whose information is being updated/added) will be operating. Flight Crew Manifest information must be submitted between 23 hours and 60 minutes prior to a given flight operation in order to ensure a security threat assessment may be conducted in a timely manner.

Flight Crew Manifest Aviation Security Threat Assessment

TSA will receive the required crewmember and, where applicable, non-crewmember Flight Crew Manifest information in advance of each scheduled flight's departure. Individuals on the manifest will be vetted each time they fly. The Flight Crew Manifest transmission for TSA crew vetting also satisfies CBP's requirements for crew manifest submissions. If incorrect or incomplete information is received, TSA will ask the aircraft operator for the correct information. TSA will conduct the aviation security threat assessment by running the names against the TSA maintained Master Crew Lists and against terrorist related and appropriate criminal databases. The results of the checks are reviewed by TSA personnel for quality assurance and determinations. The purpose of the additional checks is to add a layer of protection for those individuals who may be affected by the threat assessment process and to reduce as much as possible the number of "false positives" that may affect individuals whose names are submitted for the threat assessment. Any individual who TSA determines poses or is suspected of posing a security threat will not be authorized to be a crewmember or, where applicable, non-crewmember and TSA will share their information with the appropriate law enforcement and/or intelligence agencies, the carrier making the submission for the crewmember, and upon its request, the host government.

Master Crew List

All crewmember and non-crewmember information will be consolidated into a Master Crew List (i.e., database). As previously mentioned, this Master Crew List will be used as a vetting or reference tool when flight manifests are submitted for individual flights, meaning that each individual on the manifest will be vetted each time they fly. The TSA-maintained Master Crew Lists will include information on individuals whose names were submitted by air carriers/operators and whether they have been authorized or not authorized to be a crewmember or, as applicable, non-crewmember as determined by TSA. Before an individual's information is stored in the TSA maintained Master Crew Lists, however, a security threat assessment will be performed in a manner similar to that described above for crewmember and, where applicable, non-crewmember information contained in Flight Crew Manifests.

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

Information in TSA's system is safeguarded in accordance with the Federal Information Security Management Act of 2002, (Public Law 107-347), which established government-wide computer security and training for all persons associated with the management and operation of Federal computer systems. Additionally, the system is managed in accordance with applicable TSA and DHS automated systems-security and access policies. The computer system from which records could be accessed is policy-and security-based; access is limited through user identification and password protection to those individuals who require it to perform their official duties. All data transferred on memory sticks is encrypted for security. The system also maintains a real-time auditing function of individuals who access the system.

TSA employs the following technical safeguards to secure data:

- Filters are in place to prevent TSA from receiving more personal information than TSA requires.
- Use of advanced encryption technology to prevent internal and external tampering of TSA and CBP data and transmissions.
- Secure data transmission, including the use of password protected e-mail for sending files containing sensitive information to prevent unauthorized internal and external access.
- Password protection for files containing personal or security threat assessment data to prevent unauthorized internal and external access.
- Network firewalls to prevent intrusion into DHS network and databases.
- User identification and password authentication to prevent access to security threat assessment systems by unauthorized users.
- Security auditing tools to identify the source of failed system access attempts by unauthorized users and the improper use of data by authorized operators.
- Extensive vulnerability assessments, risk analysis and process auditing to ensure compliance with applicable federal policies and procedures and federal regulatory automated information systems requirements.
- Restricting access to the system to only those TSA personnel (government and contractor) with a strict need to know and appropriate clearances.

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

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

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

FOR QUESTIONS OR COMMENTS, PLEASE CONTACT:

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

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