Privacy Impact Assessment
for the

Air Cargo Security Requirements

April 14, 2006

Contact Point:

Pamela Hamilton
Director, Air Cargo Programs
Transportation Security Administration
571.227.2623

Reviewing Official:

Maureen Cooney
Acting Chief Privacy Officer
U.S. Department of Homeland Security
202.772.9848

Air Cargo Security Overview

Under the Aviation and Transportation Security Act (ATSA) and authority delegated from the Secretary of Homeland Security, the Assistant Secretary of Homeland Security for the Transportation Security Administration (TSA) has "the responsibility for security in all modes of transportation…."[1] As part of this responsibility, TSA is required to provide for screening cargo that will be carried aboard a passenger aircraft; and establish a system to screen, inspect, or otherwise ensure the security of all cargo that is to be transported in all-cargo aircraft as soon as practicable.[2]

Pursuant to its authority, TSA is currently publishing an air cargo security final rule (FR) that will significantly enhance air cargo security requirements. The FR significantly enhances air cargo security while preserving, to the fullest extent possible, the efficiency and timeliness of air cargo operations.

This Privacy Impact Assessment (PIA) explains that pursuant to the FR for Air Cargo Security Requirements, TSA will collect and retain personal information about four sets of individuals. The first set consists of certain individuals who have, or are applying for, unescorted access to air cargo. TSA requires employees and agents of certain aircraft operators and foreign air carriers (collectively referred to as "air carriers" in this PIA), and certain owners of an indirect air carrier (IACs) to comply with the security threat assessment requirements.[3] The second set consists of each individual who is a sole proprietor, general partner, officer or director of an IAC or an applicant to be an IAC, and certain owners of an IAC or an applicant to be an IAC. The third set consists of known shippers who are individuals. TSA will collect information on these individuals to create a database consisting of all approved "known shippers" for IAC and air carrier use. The fourth set consists of individuals who in addition to having unescorted access to cargo have responsibilities for screening cargo under 49 CFR 1544. TSA will require a fingerprint-based criminal history records check (CHRC) and name-based checks for this last set of individuals. The CHRC requirements for individuals screening cargo under 49 CFR 1544.229 are the same as the requirements for individuals with unescorted access authority to Security Identification Display Area (SIDA).
Individuals with unescorted access to a SIDA already undergo these checks and are covered under a separate PIA published in June 15, 2004, entitled "Security Threat Assessment for SIDA and Sterile Area Workers."

The TSA Office of Transportation Vetting and Credentialing (OTVC) is the office within TSA that is responsible for conducting name-based and fingerprint based checks on SIDA

[1] 49 U.S.C. § 114(d).
[2] 49 USC §§ 44901(a) and (f).
[3] These provisions apply to aircraft operators under 49 C.F.R. § 1544.101(a), to foreign air carriers under 49 C.F.R. § 1546.101, and to indirect air carriers under 49 C.F.R. part 1548. Individuals who have successfully completed either a criminal history records check under 49 C.F.R. §§ 1542.209, 1544.229, or 1544.230, or another security threat assessment approved by TSA, are not required to meet these requirements.

and Sterile Area Workers. Additionally, the OTVC implements policies associated with airport secure areas and provide support to the airport and airline security officers who adjudicate the results of the criminal history checks. Consequently, the OTVC interfaces regularly with the American Association of Airport Executives (AAAE), airport and airline industry personnel, the Federal Bureau of Investigation (FBI), U.S. Immigration and Customs Enforcement (ICE), and other federal, state, and local law enforcement entities in carrying out these responsibilities.

This PIA provides further detail about the collection of personally identifiable information for the purpose of conducting assessments on these sets of individuals to enhance the security of the air cargo supply chain. It will be modified as necessary and republished to reflect future changes and updates to the program. The nature of personal information TSA collects will vary depending on the set of individuals.

This PIA, conducted pursuant to the E-Government Act of 2002, P.L. 107-347 in accordance with 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 in accordance with the Privacy Act system of records notice, Transportation Security Threat Assessment System (DHS/TSA 002), which was published in the Federal Register on September 24, 2004, and amended on December 10, 2004. It can be found at 69 Fed. Reg. 57348, 57349 and at 69 Fed. Reg. 71837.

Definitions

Indirect Air Carrier (IAC) –Means any person or entity within the United States not in possession of an FAA air carrier operating certificate, that undertakes to engage indirectly in air transportation of property, and uses for all or any part of such transportation the services of an air carrier. This does not include the United States Postal Service (USPS) or its representative while acting on the behalf of the USPS. This definition is codified at 49 CFR § 1540.5.

Individuals Who Are Required to Screen Cargo – Means employees or agents of aircrafts with a full program (49 CFR § 1544.101(a)) or full air cargo program 49 CFR § 1544.101(h)) who the aircraft operator authorizes to fulfill its security responsibility for cargo screening. Covered aircraft operators must comply with cargo screening requirements under 49 CFR § 1544.205 and accompanying security program requirements.

Known Shipper – Means an entity or individual that an IAC or air carrier has validated according to TSA requirements in order to ship cargo on a passenger aircraft. Virtually all known shippers are corporate entities; however, individuals may also qualify. Covered IACs and air carriers must comply with the known shipper program requirements under 49 CFR §§ 1544.239, 1546.215, and 1548.17.

Security Threat Assessment (STA) – Means a name-based background check conducted by TSA using domestic and international databases to determine the existence of indicators of potential threats to national security, transportation security, or of terrorism. Covered IACs and air carriers must comply with security threat assessment requirements under 49 CFR part 1540 subpart C, and §§ 1544.228, 1546.213, 1548.15, and 1548.16.

Unescorted Access to Cargo – Means the authority granted by an aircraft operator or IAC to individuals to have unimpeded access to air cargo. This definition is codified at 49 CFR § 1540.5.

Section 1.0 System Overview

1.1 Who is affected by the collection of this data?

This data collection affects:

1. Individuals with unescorted access to air cargo.
2. Individuals who are sole proprietors, general partners, officers, directors, and certain owners of an IAC or an entity applying to be an IAC.
3. Individuals who an air carrier or indirect air carrier has qualified or validated as a known shipper.
4. Individuals who have responsibility for screening cargo that will be carried on an aircraft of an aircraft operator required to screen cargo under 49 CFR part 1544.

1.2 What personal information will be collected?

TSA will collect and retain the following information for a security threat assessment for an individual with unescorted access to cargo; each individual who is a general partner, officer or director of an IAC or an applicant to be an IAC, and certain owners of an IAC or an applicant to be an IAC; and an individual who has responsibility for screening cargo that will be carried on an aircraft of an aircraft operator required to screen cargo under 49 CFR part 1544:

1. Legal name, including first, middle, and last; any applicable suffix; and any other names used.
2. Current mailing address, including residential address if different than current mailing address, and all other residential addresses for the previous five years and email address, if applicable.
3. gender
4. Date and place of birth.
5. Social security number (although provision of one's social security number is voluntary, failure to provide a social security number may result in delays in processing the security threat assessment).

6. Citizenship status and date of naturalization if the individual is a naturalized citizen of the United States.
7. Alien registration number, if applicable.

For the second set of individuals listed above, TSA also will collect and retain a signed statement indicating whether the individual has been a sole proprietor, general partner, officer, director, or owner of an IAC that had its security program withdrawn by TSA. This statement will deter individuals whose IAC status was revoked from circumventing the verification process by joining, creating or incorporating a new or different IAC.

Under the known shipper program, TSA will collect identifying information to build a database for shippers who use indirect air carriers and air carriers and have qualified to ship cargo on passenger aircrafts. While most known shippers are corporate entities, TSA recognizes that some individuals may also be qualified as known shippers. The information collected for these individual known shippers consists of:

1. Legal name, including first, middle, and last; any applicable suffix; and any other names used.
2. Current physical address.
3. Phone number.

In addition to providing TSA with the information specified above, individuals who work for aircraft operators and who have the responsibility to screen cargo must undergo a CHRC. The FR requires that these individuals must complete a SF-57 form, a fingerprint application. The individual then submits the application through their employer to the American Association of Airport Executive's (AAAE) Transportation Security Clearinghouse. AAAE converts paper fingerprint submissions into an electronic format if the employer does not have the capacity to do so. This service limits the number of unreadable prints and facilitates a more efficient turn-around time for adjudication. AAAE sends this information to TSA via secured e-mail. TSA then transmits the fingerprint to the FBI for CHRC. The FBI returns the results to TSA's secure Fingerprint Results Distribution website for adjudication. The FBI will make a notation that the fingerprint record has been audited and the FBI may retain a copy of the fingerprints if the copy that TSA provided is more readable than the one on record.

In addition to the above information required to provide the appropriate screening function, TSA may collect and maintain information that an individual chooses to submit in connection with an appeal of a TSA determination, such as letters from a prosecutor, documents from a board of pardons, police documents, or other such relevant documents.

1.3 Why is personal information being collected and what is its intended use?

The information is being collected in order to carry out TSA's statutory mandate to secure the air cargo supply chain. IACs and air carriers are critical links in ensuring that cargo being transported in aircraft is secure and originates from a known shipper. TSA uses the

information provided in order to conduct security threat assessments on employees and agents of IACs and air carriers who have unescorted access to cargo to determine whether they pose a security risk. Furthermore, TSA will conduct the same validation process with IAC sole proprietors, general partners, officers, directors, and certain owners who control the operations of these companies. Finally, TSA has entered into a contract with the Dun & Bradstreet Government Services Group (D&B) to verify the existence and legitimacy of the IAC as a business entity.

Through the IACs and air carriers, TSA will collect limited information on known shippers to be included in a database of all known shippers. This database eliminates the need for IACs and air carriers to repeatedly input the information of a known shipper if that known shipper has been previously qualified by other IACs or air carriers. Additionally, TSA has entered into a contract with the D&B to verify the existence and legitimacy of the known shipper as a business entity.

Finally, TSA requires individuals who work for aircraft operators and who have responsibility to screen cargo to undergo a fingerprint-based criminal history records check (CHRC) to identify whether they have been convicted of a disqualifying crime, such as interference with air navigation, aircraft piracy, espionage, or any of the other enumerated crimes listed at 49 CFR § 1544.229(d). TSA also requires that these individuals undergo name-based background checks conducted by TSA using domestic and international databases to ensure that they do not pose a security risk. TSA will run this information through terrorist-related and immigration databases it maintains or uses. Any application that meets the minimum criteria established by TSA as a possible match will undergo further analysis. TSA may also transmit the information to ICE for immigration status checks using its additional resources. If a potential or actual immigration violation is identified, ICE may initiate subsequent investigative action. Upon the conclusion of any ICE investigative action, ICE will forward the results to TSA for review.

1.4 What information technology system will be used for this program and how will it be integrated into a step-by-step process?

A database is being developed in TSA's Indirect Air Carrier Management System (IAC MS) that will enable electronic submission by the IAC of data required for a name-based security threat assessment. TSA will conduct the same validation process with IAC sole proprietors, general partners, officers, directors, and certain owners who control the operations of these companies. TSA will run this information through terrorist-related and immigration databases it maintains or uses. Any application that meets the minimum criteria established by TSA as a possible match will undergo further analysis. TSA will run the information transmitted through Federal databases, including the Terrorist Screening Center Database (TSDB), National Crime Information Center (NCIC), TSA watch lists, and immigration data systems. TSA may also transmit the information to Immigration and Customs Enforcement (ICE) for immigration status checks using its additional resources. If a potential or actual immigration violation is identified, ICE may initiate subsequent investigative action. Upon the conclusion of any ICE investigative action, ICE will forward

the results to TSA for review. Finally, TSA will run a check of the IAC through D&B to check whether the IAC is a legitimate business entity.

For the Known Shipper Program, TSA has developed a web-based program so that IACs and air carriers can input known shipper information, as specified above. This database will be used solely by an IAC or air carrier to check whether the shipper wishing to transport cargo on a passenger aircraft is an existing known shipper. TSA has a contract with D&B to verify the existence and legitimacy of the known shipper as a business entity. Individual known shippers in the database would also be subject to this vetting. Finally, aircraft operators must ensure that their employees and agents with responsibilities to screen cargo have not been convicted of a disqualifying criminal offense as set forth in 49 CFR § 1544.229(d).

The process for the fingerprint-based criminal history records checks is as follows. AAAE consolidates the fingerprints and accompanying personal information from the air carrier and provides it to TSA's Office of Vetting and Credentialing (OTVC). OTVC forwards the fingerprint application to the FBI who runs the prints through the Criminal Justice Information System. OTVC will also run the personal information through federal databases, including the TSDB, TSA watch lists, immigration and commercial and public data systems. Results from the FBI check are provided back to TSA for adjudication, and TSA posts the results on a secure, password protected website. Air carrier security contacts are provided only with access to view the results of their own employees and agents. The posting will be limited to whether the individual is approved, pending, or denied. For all applicants, TSA will retain basic personal information consisting of name, address and date of birth. For individuals who are denied; TSA will retain all information, including the basis for the denial.

TSA will also do additional name-based checks on these individuals. As described above, TSA will run the information transmitted through federal databases, including the Terrorist Screening Center Database (TSDB), National Crime Information Center (NCIC), TSA watch lists, immigration databases, including Systematic Alien Verification for Entitlements (SAVE) Program. TSA may also transmit the information to ICE. If a potential or actual immigration violation is identified, ICE may initiate subsequent investigative action. Upon the conclusion of any ICE investigative action, ICE will forward the results to TSA for review.

1.5 What databases will the names be run against?

For security threat assessments, TSA will run names against federal databases, including NCIC, TSDB and TSA watch lists, to identify potential threats to aviation security. In addition, TSA will verify this information through immigration, commercial and public databases. These are national databases used by government agencies to determine and deter potential security threats and terrorist activity.

For approval to operate under an IAC security program, TSA currently has a contract with a commercial database to verify that the IAC is a legitimate corporate entity, and may use this contract to verify information about individuals.

For the known shipper database, TSA has a contract with D&B to verify the existence and legitimacy of known shipper business entities included in the TSA known shipper database. Individual shippers who are included in the known shipper database would also be subject to that vetting. D&B will validate the existing TSA-managed known shipper database (currently containing approximately 400,000 records) and match these against its business and corporate referential databases. D&B will verify the existence of the company utilizing data elements such as Company Name, Address, and Telephone Number, and return data including the DUNS Number, Standard Industrial Classification (SIC), Year Started, Import Indicator, Out of Business Indicators, Suits/Liens/Judgments, and Corporate Linkage information**.** Business Risk Scores and Identity Verification (Patriot Act Compliance) information will also be appended. This file will be monitored daily for significant changes within the database with file refreshes completed on a monthly basis.

TSA sends CHRC fingerprints to the FBI where a criminal history records check is performed.

Section 2.0 Notice

2.1 What opportunities for consent are provided to individuals regarding the collection of their personal data and information?

TSA will provide a written Privacy Act Notice to individuals at the time the individual's information is collected.[4] This notice is required by the Privacy Act of 1974, as amended (5 U.S.C. 552a (e)(3)) and will inform candidates why their personal information is being collected, the authority for the collection, and how it will be used. The notice will also inform the individual that provision of their personal information for purposes of the security threat assessment is voluntary. However, failure to supply this information could have consequences on unescorted access or approval to operate as an IAC.[5]

Air carriers and IACs must provide individuals qualified as known shippers with the written Privacy Act Notice prior to entering their information into the known shipper database. Failure to supply this information could result in an individual not being allowed to ship cargo on a passenger aircraft. TSA will perform routine audits as part of the IAC and air carrier regulatory compliance program to ensure compliance.

Finally, air carriers must provide individuals who must undergo a CHRC with a Privacy Act Notice prior to collecting fingerprints and personal data. Again, failure to supply this

[4] IACs, and not the shipper, would enter the candidate's information on the website.
[5] Although provision of one's social security number is voluntary, failure to provide a social security number may result in delays in processing the security threat assessment.

information could have consequences on whether an individual could screen cargo under 29 CFR part 1544. TSA is regularly in communication with AAAE to ensure that the privacy act notice is given to individuals prior to gathering any information.

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

No. The information collected for the security threat assessment and the CHRC is part of an existing TSA Privacy Act system of records known as the Transportation Security Threat Assessment 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.

Section 3.0 Information Sharing

3.1 With whom will the collected information be shared?

The information will be shared with the appropriate DHS personnel and contractors involved in the program and other government agencies who are involved in processing the name-based security threat assessments and CHRCs. In addition, this information may be provided to other federal agencies to perform immigration status checks. The collection, maintenance, and disclosure of information will be conducted in compliance with the Privacy Act and the published system of records notice. TSA reserves the right to report to employers, local law enforcement or other federal agencies adverse or derogatory results from security threat assessments performed on IAC and air carrier employees and agents who seek unescorted access to air cargo, security threat assessments performed on individuals who are sole proprietors, general partners, officers, directors, and certain owners of an IAC or an applicant to be an IAC, and CHRC and background checks for individuals who have responsibility for screening cargo that will be carried on an aircraft of an aircraft operator required to screen cargo under 49 CFR part 1544.

Individuals who receive a negative determination of his or her security threat assessment will not be permitted to have unescorted access to air cargo nor will he or she be allowed to fulfill the position of sole proprietors, general partners, officers, directors, and certain owners of an IAC. TSA reserves the right to share adverse information with other law enforcement agencies for security and law enforcement purposes only.

Air carriers and IACs have access to the known shipper database, which contains a list of all entities, including individuals, who have met criteria detailed in their TSA-approved security programs and therefore can ship cargo from shippers in the database on a passenger aircraft. However, regulated entities with access to this password protected database cannot search the database to mine it for known shipper identities, and will not be able to produce the entire list of known shippers in a single query. Rather, regulated entities will only be able to confirm the status of a particular shipper participating in the known shipper program. Air carriers and indirect air carriers will be advised, at the time

each query is made, that the use of the information contained in the query results is strictly restricted to the verification of the known shipper status and may not be shared, sold or otherwise distributed to other parties. Aircraft operators are prohibited from transporting cargo on passenger aircrafts from a shipper that is not approved for known shipper status. All IACs undergo routine audits to ensure that only cargo from an approved known shipper is transported on passenger aircrafts.

Finally, individuals who have a disqualifying criminal offense or who receive a negative determination on the additional name-based security check will not be allowed to screen cargo that will be carried on an aircraft of an aircraft operator required to screen cargo under 49 CFR part 1544.

Section 4.0 Individual Redress and Correction

TSA offers the following redress and correction procedures for covered individuals:

1. Individuals with unescorted access to air cargo, or who are sole proprietors, general partners, officers, directors, and certain owners of an IAC –

If TSA determines that the individual poses a security threat, then it will issue an Initial Determination of Threat Assessment to the individual and the employer. The determination includes a statement that TSA has determined that the individual poses, or is suspected of posing, a security threat; the basis for the determination; the process by which the individual may appeal the determination; and a statement that if the individual chooses not to appeal TSA's determination within 30 days of receipt of the Initial Determination of Threat Assessment, or does not request an extension of time within 30 days of the Initial Determination of Threat Assessment in order to file an appeal, the Initial Determination of Threat Assessment becomes final.

An individual may appeal an Initial Denial of Authorization for Unescorted Cargo Access if the individual asserts that he or she does not pose a security threat. An individual may initiate an appeal by submitting a written reply or written request for materials from TSA. If the individual fails to initiate an appeal within 30 days of receipt of the Initial Denial of Authorization, the Initial Denial becomes final, and TSA will serve a Final Denial of Authorization for Unescorted Cargo Access on the operator and the individual.

An individual who receives an Initial Denial of Authorization for Unescorted Cargo Access may serve upon TSA a written request for copies of the materials upon which the Initial Denial of Authorization was based. TSA will not include any classified information or other protected information in responding.

If the Initial Denial of Authorization for Unescorted Cargo Access was based on a record that the individual believes is erroneous, he or she may correct the record by contacting the jurisdiction or entity responsible for the information and attempting to correct or complete information contained in his or her record. The individual must then provide

TSA with the revised record, or a certified true copy of the information from the appropriate entity, before TSA may determine that the individual meets the clearance standards for the Security Threat Assessment. Individuals who believe that their immigration status check determination is inaccurate should contact ICE to address their concerns.

For purposes of judicial review, the Final Determination of Threat Assessment constitutes a final TSA order in accordance with 49 U.S.C. 46110.

1. Individuals who have been validated as a known shipper by an air carrier or indirect air carrier –

TSA is not currently making any determinations that affect the individual rights for which redress is required. This database currently is used solely by an IAC or air carrier to check whether a shipper wishing to transport cargo on a passenger aircraft is an existing known shipper. However, TSA is planning to contract with D&B to verify the existence and legitimacy of the known shipper as a business entity. Individual known shippers in the database would also be subject to this vetting.

When TSA begins vetting known shippers to ensure their legitimacy, it will also offer a redress policy. When an IAC enters an individual known shipper in the database, D &B will perform a check to see if that individual is in its database. Since the D&B database does not typically include individuals, TSA will also verify that the individual is located at the address that he or she listed in a separate check. If TSA is unable to verify that the address and contact information entered by the IAC is legitimate, it will notify the IAC. The IAC will then double-check this information and resubmit when applicable. If neither TSA nor the IAC can establish that the individual's contact information is legitimate, the individual will not be determined a "known shipper" for that shipment, and will not be entered into the Known Shipper database.

1. Individuals who screen cargo that will be carried on an aircraft of an aircraft operator required to screen cargo under 49 CFR part 1544 –

TSA will adjudicate the results of the CHRC for individuals who will be screening cargo pursuant to 49 CFR § 1544.229(d). If an individual disputes the results of the CHRC (for example that the disposition of a charge(s) is incorrect), the individual may provide court documentation to TSA. Individuals may appeal to TSA to show that the disposition (or charge) does not fall under the disqualifying offense category, a corrected disposition, or that the charge no longer falls under the disqualifying offense category.

Individuals who receive a determination of threat assessment will be given the opportunity to contact TSA pursuant to 1540.207. Individuals who believe that their immigration status check determination will be given the opportunity to correct any incorrect underlying information or court records.

Section 5.0 Retention

5.1 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 would permit it to destroy these records after a determined period of time. Until NARA approves this records schedule, however, TSA does not have legal authority to dispose of these records. TSA will update its records periodically consistent with regulations that require individuals to submit to a security threat assessment.
The CHRC results are maintained by TSA on the Fingerprint Results Distribution website. TSA will need to keep this information because it formed the basis for the final adjudication decision. The individual record may be used to determine if the granting of the credential was made correctly. These records may also be used to audit the regulated entity.

Section 6.0 Security and Access

6.1 How will the information be secured against unauthorized use?

TSA will secure personal information against unauthorized use through 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. FISMA certification and accreditation will be prepared once the software programs are developed. Only TSA employees and contractors with proper security credentials and passwords, and a need to know in order to fulfill their duties associated with conducting security threat assessments, will have access to this information. 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:

- 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 U.S.C 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 (Pub. L. 107-347), which establishes minimum security practices for federal security systems.

6.2 What technical safeguards are in place to secure the data?

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

TSA employs the following technical safeguards to secure data:

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

For questions or comments, please contact:

Lisa S. Dean, Privacy Officer, Transportation Security Administration, 571-227-3947
Pam Hamilton, Air Cargo Programs, Transportation Security Administration, 571-227-2623.

Approval Signature Page

Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security