Privacy Impact Assessment
for the Tactical Information Sharing System

March 28, 2007

Contact Point
ASAC Abel Reynoso
Transportation Security Administration
Federal Air Marshal Service
Investigations Division – Tactical Information Branch
Abel.E.Reynoso@secureskies.net

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 Transportation Security Administration (TSA) operates the Tactical Information Sharing System (TISS). The Tactical Information Sharing System receives, assesses, and distributes intelligence information related to transportation security to Federal Air Marshals (FAMs) and other Federal, State, and local law enforcement.

Introduction

Section 114 of the Aviation and Transportation Security Act (ATSA) (Pub. L. 107-71, November 19, 2001, 115 Stat. 597) grants TSA the responsibility for security in all modes of transportation. Specifically, Section 114(f) grants the TSA Administrator authority to "receive, assess, and distribute intelligence information related to transportation security" as well as to "assess threats to transportation." TISS is one means by which TSA fulfills that responsibility by enabling FAMs in the field to report for analysis the observation of suspicious behavior that may signal some form of pre-operational surveillance or activity, and provide an information source for examining long-term trends and patterns. Criminal or terrorist acts that threaten transportation security are most vulnerable in the planning stages and TISS will assist in identifying such efforts.

Federal Air Marshals and other federal, state, and local officials are trained to identify and report suspicious activity while performing their daily duties. They submit Surveillance Detection Reports (SDRs) electronically into the TISS SDR database to report suspicious activities that fall below the threshold of an actionable law enforcement incident. FAMs assigned to the Tactical Information Branch (TIB) may also create SDRs based on information received in the Federal Air Marshal Service (FAMS) Activity Reports or TSA Daily Reports.

The information contained in the SDRs is manually reviewed to seek patterns or associations with other information potentially affecting aviation security. In addition, software is used to perform searches based on criteria. Currently, the software performs only name matches, but the system has the capacity to search other fields for patterns and has been used to perform queries in response to specific intelligence or apparent trends discerned in manual searches.

Other participating law enforcement organizations outside of the FAMS may have access to the TISS in order to review information contained in these reports for intelligence and security-related purposes. To facilitate such access, the FAMS have developed partnerships with other components of the Department of Homeland Security (DHS), including other divisions of the Transportation Security Administration (TSA), U.S. Immigration and Customs Enforcement (ICE), United States Coast Guard (USCG), and U.S. Customs and Border Protection (CBP), as well as with other federal entities, including the National Counterterrorism Center (NCTC), Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), and Department of Defense (DoD). In addition, the FAMS have granted access to TISS SDRs to certain local and state law enforcement entities in an effort to involve agencies that have law enforcement jurisdiction in and around airports. TISS contains sensitive law enforcement information that is accessed and shared only among law enforcement, intelligence and security agencies with an appropriate need to know.

Because this system entails a new collection of information about members of the public in an

identifiable form, the E-Government Act of 2002, Public Law 107-347 Section208, requires that TSA conduct a Privacy Impact Assessment (PIA).

Section 1.0
Information collected and maintained

1.1 What information is to be collected?

Where available and at the reasonable operational discretion of a FAM, information pertaining to suspicious activity and behavior with a nexus to the aviation domain may be compiled into an SDR, which is stored in TISS. This information is primarily activity or behavioral information but also may contain personal information regarding the individuals involved in the suspicious activity. Information fields within the SDR include general information such as time, date, airport, geographical location, and if available, photographs. Subject information collected may include: first, middle, and last names; aliases and nicknames; home and business addresses; employer information; Social Security numbers; other available identification numbers such as drivers license number or passport number; date of birth; languages spoken; nationality; age, sex and race; height and weight; eye color; hair color, style and length; and facial hair, scars, tattoos and piercings, clothing (including colors and patterns) and eyewear. Vehicle information, including make, model, model year, color, license plate, state of registry, VIN, as well as registration information may also be collected.

Although the TISS possesses the capacity to maintain each of the data elements noted above, a user is not required and would rarely have the opportunity to compile all of these data elements. FAMs only compile observable information to report activities that fall below the threshold of a law enforcement actionable incident. Additionally, a large percentage of TISS information is derived from reports that are provided to FAMs by external sources (as described in Section 1.2). These reports pertaining to suspicious activity may be translated into an SDR and entered into TISS.

1.2 From whom is information collected?

The information contained in the TISS is a combination of observations made by individual FAMs and law enforcement officials with responsibility for aviation security along with data reported by other entities within the aviation domain, such as air carriers, as well as directly from the individual in connection with an encounter with FAMs or law enforcement officials. FAMs and other TISS users record their observations of suspicious activity in SDRs and then submit the report electronically via a customized, encrypted Personal Digital Assistant (PDA) application or through the Internet, via the secure TISS web site. Members of the aviation industry, primarily aircraft crews, may submit reports of suspicious activity via electronic mail. The reports submitted via electronic mail are reviewed and investigated by FAMs in the Tactical Information Branch (TIB) and manually entered into the TISS as an SDR.

Other sources of information include the FAMS Activity Reports, the DHS Daily Operations Report, the FAMS Mission Operations Center (MOC) Daily Report, the TSA Performance and Results Information System (PARIS) Daily Report, the FBI Most Wanted List, the ICE Most Wanted List, the Office of Foreign Assets Control (OFAC) Blocked Persons List, and the National Center for Missing and Exploited Children (NCMEC) alerts. In certain instances, reports of suspicious activity derived from these sources may be

translated into an SDR by members of the TIB. In other instances, these sources of information are used for name comparison purposes and to analyze patterns and trends. The results of these comparison searches are not input into TISS.

1.3 Why is the information being collected?

This information is collected to detect, deter, and defeat a criminal or terrorist act in the aviation domain before it occurs. The information is used to identify actions, patterns, or trends that may indicate preoperational terrorist or criminal activity within the aviation domain.

1.4 How is the information collected?

Information is collected by a FAM or other law enforcement officer who directly inputs the observation into the system.

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

Section 114 of the Aviation and Transportation Security Act (ATSA) (Pub. L. 107-71, November 19, 2001, 115 Stat. 597) grants TSA the responsibility for security in all modes of transportation. Specifically, Section 114(f) grants the TSA Administrator authority to "receive, assess, and distribute intelligence information related to transportation security" as well as to "assess threats to transportation." TISS is just one means by which TSA fulfills that responsibility with respect to the FAMS. Every authorized TISS user, at the FAMS or non-FAMS law enforcement level, receives comprehensive training concerning the TISS system and the appropriate criterion of information that is eligible for system input. This includes classroom instruction, demonstrations, and for FAMs, practical exercises, with assessment from the FAMS trainers.

1.6 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

The TISS is designed to identify trend or patterns in suspicious activity. This demands a collection of as much information as possible regarding a certain event or activity, including personally identifiable information where available. Privacy risks of the individual being unaware of the collection and the amount of information are mitigated by the strict limitation of access to the system. Access is limited to law enforcement or intelligence personnel with a responsibility for aviation or transportation security. This access is described further later in this PIA.

Section 2.0
Uses of the system and the information

2.1 Describe all the uses of information.

The information is used to identify actions, patterns, or trends that may indicate preoperational terrorist or criminal activity within the aviation domain. The TIB correlates the suspicious activity received through SDRs entered into TISS with investigations and intelligence received from other tactical information resources. A software tool searches all SDRs for matching names, events, or patterns based on search criteria determined by the TIB to query TISS utilizing the number of occurrences in conjunction with defined fields. If a match occurs, TIB personnel analyze SDRs containing the match. In addition to this automated process, TIB also conducts manual searches seeking patterns.

As necessary, TIB may forward pertinent information to other units within the FAMS or to federal, state, or local entities for further analysis or informative purposes.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

TISS seeks to find patterns and trends that may indicate preoperational terrorist or criminal activity, but it does not predict behavior. The software tool currently searches for name matches but the system has been and will again be used to search other statistical parameters relevant to the transportation security.

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

The accuracy of information input into a SDR is important to support the effective use of TISS. FAM training emphasizes the importance of accurate data collection to the integrity of the system and the respect it is accorded by the law enforcement community. Information regarding behavior will be input directly by the FAM observing the conduct. For individually identifying information, the FAM may collect the information directly from the individual. When the information is collected from third parties, all users are trained to input personally identifying information that has sufficient indicia of accuracy.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

Access to the TISS is limited to law enforcement or intelligence personnel with a responsibility for transportation or national security. All users that have access to the system have unique user names and passwords, and must sign a User Account Authorization acknowledging user obligations for safeguarding materials and monitoring of use. Audits of the system are conducted periodically to ensure proper use of the system.

Section 3.0
Retention

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

Information input into TISS by a FAM or submitted by the aviation industry to the FAMS for input into TISS will be retained for twenty five (25) years from the date of last entry in accordance with a schedule which has been approved by the National Archives and Records Administration (NARA).

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

Yes. NARA approved the TISS record retention schedule in December 2005.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

Information collected through this program will be maintained for 25 years in accordance with a NARA-approved record retention schedule which ensures that the agency meets its operational requirements and furthers the FAMS mission to ensure the security of the Nation's transportation system.

Section 4.0
Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

FAMs and employees of the TSA Office of Intelligence have access to information contained in TISS. In addition, the following DHS components currently have direct access to the TISS database:

U.S. Customs and Border Protection (CBP)

U.S. Immigration and Customs Enforcement (ICE)

U.S. Coast Guard (USCG)

DHS Office of Intelligence Analysis (OIA)

Information contained in TISS 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 Privacy Act of 1974, 5 USC §552a.

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

All data within the system is shared with authorized users. The organizations with access to the system have a nexus to transportation or national security in relation to the aviation domain and have a need to know suspicious activity within that domain. Although all users have access to the data, only FAMS users have access to the full pattern/trend analysis functions of the system. TISS information, including raw data as well as reports and analysis, may be shared within DHS for intelligence, counterintelligence, law enforcement, or other official purposes related to transportation or national security.

4.3 How is the information transmitted or disclosed?

In limited situations, the information in TISS may be shared telephonically, via encrypted email, or in person. However, the system is primarily designed to require access through a secure website via the Internet or via a customized encrypted PDA application. Each user has a unique username and password used to access the system.

Currently, users have access to all records in TISS. A hierarchy system is currently being developed to limit sharing of certain information to Non-FAMS agencies.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

TSA will limit its sharing of the information to those DHS officials, employees, and contractors of DHS who have a need for the record in performance of their duties. Access to the full pattern/trend analysis functions is limited to FAMs. DHS Employees may be subject to discipline and administrative action for unauthorized disclosure of this information. Privacy protections include strict access controls, including passwords and real-time auditing that tracks access to electronic information.

Section 5.0
External sharing and disclosure

5.1 With which external organizations is the information shared?

The following is a list of the agencies/departments that currently have access to the information in TISS:

- Allegheny County, PA Police
- Bangor, ME Police
- Broward County, FL Police

- Burbank Airport Police
- Butler Township, OH Police
- Central Intelligence Agency (CIA)
- Charlotte Douglas Airport Police
- Charlotte-Mecklenburg Police
- Cincinnati / N. Kentucky International Airport Police
- Colorado Springs Airport Police
- Dayton Airport Police
- Defense Intelligence Agency (DIA)
- U.S. Department of Defense (DoD)
- U.S. Department of State
- U.S. Department of Transportation (DOT)
- Des Moines, IN Police
- Fairfax County, VA Police
- Federal Bureau of Investigation (FBI)
- Indianapolis Airport Police
- Kansas City Airport Police
- Lee County Port Authority Police
- Lincoln Airport Police
- Los Angeles County Sheriff
- Los Angeles Police
- Los Angeles World Airport Police
- Louisville, KY Metro Police
- Massachusetts State Police
- Miami-Dade Police
- Minneapolis / St. Paul International Airport Police
- Metropolitan Washington Airports Authority (MWAA) Police Department
- National Counterterrorism Center (NCTC)

- National Ground Intelligence Center (NGIC)
- North American Aerospace Defense Command (NORAD)
- New York Police Department (NYPD)
- Ohio State Patrol
- Omaha Airport Authority Police
- Orlando Police Department – Airport Division
- Philadelphia Police
- Piedmont-Triad Airport Police
- Port Authority of NY/NJ
- Port Columbus Airport Police
- Port of Seattle Police
- Raleigh Durham Airport Police
- San Diego Airport Authority Police
- San Francisco Police
- San Mateo County Sheriff
- Tampa International Airport Police
- Terrorist Screening Center (TSC)
- Vandalia, OH Police
- Virginia State Police

This listing may be periodically updated to reflect additional entities that may utilize this system in the future. Information in TISS may also be shared with other Federal, state, or local law enforcement entities pursuant to the Privacy Act and in accordance with the routine uses identified in the applicable Privacy Act system of records notice (SORN), DHS/TSA001, Transportation Security Enforcement Records System. This SORN was last published in the Federal Register on December 10, 2004, and can be found at 69 FR 71828, 71839.

5.2 What information is shared and for what purpose?

Only authorized users may access TISS. Although all users have access to the raw data in TISS and can perform simple searches (such as incidents relating to their specific airport), only TSA users have access to the full trend analysis functions of the system. The external organizations with access to the system have a nexus to transportation or national security in relation to the aviation domain and have a need to know

suspicious activity within that domain. This information is used to support aviation security.

5.3 How is the information transmitted or disclosed?

In limited situations, the information in TISS may be shared telephonically, via encrypted email, or in person. However, the system is designed to require access through a secure website via the Internet or via a customized PDA application.

A hierarchy system is currently being developed to limit sharing of certain information to Non-FAMS agencies because of privacy or other concerns.

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. Each individual accessing the system executes a user agreement, binding the user to the requirements of the TISS. In addition, the Privacy Act System of Records notice described above provides the necessary allowances for sharing of the information in accordance with the Privacy Act.

5.5 How is the shared information secured by the recipient?

Any federal agency receiving this information is required to handle and secure the information in accordance with the Privacy Act and their applicable SORNs, as well as User Agreements that require users to properly safeguard and restrict access to information in TISS to authorized users only. All information in TISS is marked as law enforcement sensitive.

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

Outside users receive training in how to access and use the system from Federal Air Marshals assigned to the FAMS Office of Training and Development. All non-FAMS users are required to sign a TISS User Agreement and all non-DHS users must execute a Non-disclosure Agreement prior to being granted access to the system. 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: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

FAMS will share this information under the applicable provisions of the System of Records Notice (SORN) and the Privacy Act. All non-FAMS users are required to sign a TISS User Agreement and all non-DHS users must execute a Non-disclosure Agreement which prohibits disclosure of information except to persons authorized by the FAMS prior to being granted access to the system. Non-FAMS users do not have

access to the full pattern/trend analysis functions. By limiting the sharing of this information, FAMS is mitigating any attendant privacy risks.

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?

No. Much of the information in the TISS consists of FAM's observations of suspicious activity, as the information is gathered when a FAM observes the actions of the subject. The FAM generally has no prior knowledge that the activity is going to occur, therefore has no ability to give notice that the information is going to be gathered. Personally identifiable information will not be collected in all cases as a result of a FAM's observation. There is no opportunity to provide prior notice concerning information compiled from third party sources.

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

Information contained in TISS is generally not gathered directly from an individual, but consists of the observations of a FAM. Generally, because the information is based on observations and not interviews or other techniques used to gather information directly from an individual, persons whose information is contained in the system in an identifiable form would not have an opportunity to decline to provide information. A FAM may make contact with an individual and conduct a voluntary law enforcement interview.

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?

No. Since an individual's name or other personal information may be obtained from third party sources, such as an airline or a non-FAM report, the individual is not provided an opportunity to consent to particular uses of the information. In addition, if a FAM engages an individual in conversation and the individual voluntarily provides his or her name, the individual is making a choice to provide that information.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Information in the TISS is typically based on FAM observations and often does not involve interaction with the subject of the record. If a FAM does make contact with an individual and conducts a law enforcement interview, the individual may decline to provide information.

Section 7.0
Individual Access, Redress and Correction

7.1 What are the procedures that allow individuals to gain access to their own information?

While much of the information in the system is exempt from release under the FOIA and Privacy Act, individuals may request access to their information pursuant to the applicable provisions of the Privacy Act and the DHS Privacy Act regulation at 6 CFR Section 5.21 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, West 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, current address, date and place of birth, telephone number, and email address (optional). Privacy Act requesters must either provide a notarized and signed request or sign the request pursuant to penalty of perjury, 28 U.S.C. §1746. Please refer to the TSA FOIA web site (http://www.tsa.gov/public).

7.2 What are the procedures for correcting erroneous information?

To the extent record access is granted under the FOIA or Privacy Act, individuals may request correction of their personal information in this system of records in accordance with the applicable provisions of the Privacy Act and the DHS Privacy Act regulation at 6 CFR Section 5.26.

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

DHS has published procedures to request amendment of records at 6 CFR Section 5.26.

7.4 If no redress is provided, are alternatives available?

Individuals may request access or amendment of their records in TISS in accordance with the applicable provisions of the Privacy Act and the DHS Privacy Act regulation at 6 CFR Section 5.21.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

Individuals may request access to and amendment of their personal information contained in this system in accordance with the Privacy Act and the DHS Privacy Act regulation, however, much of the information in the system is exempt under the FOIA and Privacy Act as law enforcement or intelligence information, and may also be Sensitive Security Information exempt from disclosure under 49 USC §114(s).

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.)

Only Office of Law Enforcement/Federal Air Marshal Service employees have general access directly to the TISS. This includes system administrators, security administrators, FAMs, and other persons within TSA who have a need to access the system or information contained in the system in the performance of their duties. Personnel from other selected law enforcement or intelligence agencies with a nexus transportation or national security will have access to SDRs and reports. (See Section 5.1 for a list of organizations that have access to TISS).

8.2 Will contractors to DHS have access to the system?

Yes. Contractors have access to the system for system maintenance and security assessments, but not as TISS users. Contractors have signed appropriate non-disclosure agreements and agreed to handle the information in accordance with the Privacy Act of 1974, as amended.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes, security roles/privileges are used to determine who has access to pattern/trend analysis, editing, and report generator functions of the system. Currently, users have access to all information in TISS, but only FAMS users have access to the pattern/trend analysis functions of the system. Although all users have access to all data in the system, procedures are under development to limit access based on criteria, such as the user's organization. When implemented, the FAMS will have the ability to designate hierarchy levels that will allow controlled access to different information within the system. Each report contained in the system includes a report history.

8.4 What procedures are in place to determine which users may access the system and are they documented?

The decision authority of when to create an account, and for whom, rests with the TIB. Generally, user accounts are granted for members of agencies with a law enforcement or intelligence nexus to transportation security in the aviation domain.

Access privileges to the TISS are documented using the TISS User Account Authorization form, which is retained by the TIB.

In addition to the TISS User Account Authorization form, new users that are not employed by DHS are required to submit a DHS Non-Disclosure Form and a TIB Non-Disclosure form. Both of these forms are maintained by the TIB.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Each SDR in the system has a time stamp tracking history. The history documents all persons who have viewed, edited, or printed the report including the date, time, and field office of the user.

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

Systematic network and system monitoring is in place to detect intrusions. Role-based security is used to prevent unauthorized use of the information, including improper printing or editing of data.

TSA Office of the Chief Information Security Officer (OCISO) performed a formal risk assessment on the TISS system against the information asset 'data', i.e., the information held within the TISS system, in accordance with NIST Special Publication, 800-30, Risk Management Guide for Information Technology Systems. A formal risk assessment was completed by the TSA OCISO on July 24, 2006. In addition, the OLE-FAMS completed a NIST 800-26, Security Self Assessment, on June 13, 2006. The risk assessment and Security Self Assessment will be completed annually.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

Non-FAMS users are given training by the FAMS instructors on the use of the system and the use of law enforcement sensitive information found within the database. The FAMS personnel are required to complete the required TSA information technology (IT) security and privacy training.

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

Information in the TISS 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. Authority to Operate was granted on August 9, 2006.

This system, including the contractor facility that houses the server, will employ security controls developed in accordance with FIPS 199 and NIST SP 800-53 standards. The system is being assessed for security risks and follows the DHS/TSA IT Security Policies and Procedures consistent with statutory, regulatory, and internal DHS guidance. This system will be certified in accordance with NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems. An annual self-assessment will be conducted in accordance with FISMA utilizing SP 800-26, Security Self-Assessment Guide for Information Technology Systems. In addition, the contractor operates the TISS system in accordance with DTFACT-03-D-00030 /DTFACT-03-R-00020. The system is FISMA compliant, and appropriate reviews to ensure compliance are planned. Data transmitted via the PDA is encrypted in-transit via SSL and VPN, and data is stored in at destination in encrypted format.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Data on the TISS system is secured in accordance with applicable federal standards, including systematic network and system monitoring is in place to detect intrusions. Security controls are in place to protect the confidentiality, availability, and integrity of the data, including role-based access controls to that enforce a strict need to know policy. Each user is given a unique login name and password and audit trails are maintained and monitored to track user access and detect any unauthorized use. All TISS system users must sign a user agreement. In addition, all individuals outside of DHS who are granted access to the TISS system are required to sign a DHS Non-Disclosure agreement.

Section 9.0 Technology

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

The Tactical Information Sharing System was built from a combination of Commercial Off the Shelf (COTS) software & hardware and some customized software developed specifically for TISS.

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

Servers are built to DHS guidelines. A FIPS 199 was completed in December 2005 and authority to operate was granted in August 2006. This system completed a FIPS 199 to ensure the categorization of the data is accurately and appropriately labeled and secured. Security and privacy requirements were derived based on the sensitivity category of the system, which is considered to be HIGH sensitivity. The high baseline requirements reflect that stringent controls are necessary for protecting the confidentiality, integrity, and availability of the data in this system. The system is designed to support the high baseline requirements and protects the integrity and privacy of personal information.

9.3 What design choices were made to enhance privacy?

Access to the system is strictly controlled and limited according to the organization's and individual's need to know the information in to perform their duties. As noted above, systematic network and system monitoring is in place to detect intrusions Each SDR in the system has a time stamp tracking history listing all persons who have viewed, edited, or printed the report including the date, time and field office of the user. All information in the system is secured in accordance with Federal standards, including FISMA.

Conclusion

TISS enables FAMs in the field to report the observation of suspicious behavior and activity instantly into the TISS database for analysis, and provide an information source for examining long-term trends and patterns. With this information, FAMs are equipped to stop criminal or terrorist acts that threaten transportation security when they are most vulnerable - in the planning stages of an operation. Although the TISS was designed with the purpose of sharing suspicious activity reporting with numerous agencies for purposes of transportation or national security, adherence to applicable privacy and security requirements is mandated in order to ensure proper handling and sharing of information in accordance with the applicable provisions of the Privacy Act and the SORN. All physical storage of information is maintained in a central location that meets or exceeds DHS IT and physical security standards and access to the system and its records is limited to those agencies and individuals with a need to know the information to perform their official duties. The TISS is at the forefront of the fight against terrorist within the aviation domain through the identification of preoperational activity using suspicious activity reporting. While

maintaining the mission to protect the citizens of the United States and to promote confidence in the aviation industry, the Office of Law Enforcement/Federal Air Marshal Service will continue to protect and appropriately use the information that makes this effort possible.

Responsible Officials

ASAC Abel Reynoso
Federal Air Marshal Service, Tactical Information Branch – Investigations Division
Transportation Security Administration

Abel.E.Reynoso@secureskies.net

Approval Signature Page

_____

Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security