Privacy Impact Assessment
for the

Transportation Security Administration Enterprise Performance Management Platform (EPMP)

DHS/TSA/PIA-034

May 10, 2011

Contact Point
James Watts
Operational Process & Performance Metrics
Transportation Security Administration
Jim.Watts@dhs.gov

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Transportation Security Administration (TSA) Enterprise Performance Management Platform (EPMP) is designed to assist in performing security management functions using a wide variety of data associated with security, equipment, and screening processes from TSA's security activities. EPMP will now maintain personally identifiable information (PII) about members of the public in excess of basic contact information, which requires TSA to conduct a new Privacy Impact Assessment (PIA). This PIA focuses on the portions of EPMP using PII.

Overview

EPMP is principally used to generate statistical and operations management information (such as equipment maintenance, property tracking, number of enplanements, employee service information). EPMP previously maintained only limited PII (contact information on members of the public) and thus was covered by the Department of Homeland Security General Contact Lists Privacy Impact Assessment.

EPMP uses data from a variety of sources to generate performance information. The principal application within EPMP is the Performance Information Management System (PIMS), which is both a business tool and a data warehouse. Principal data sources within the PIMS data warehouse include the Airport Information Management (AIM) system and Performance Measurement Information System (PMIS). AIM is an application that assists facilities in managing day-to-day activities and includes a variety of employee and equipment information. PMIS is a data entry source for a variety of TSA metrics associated with security activities (such as screening throughput, number of prohibited items intercepted, security drills, wait times, number of checkpoints and lanes, and machine resources). PMIS will also be used to securely communicate information, that is currently passed by e-mail, to TSA field personnel regarding individuals transiting through their airport who are under special travel arrangements, and individuals identified in the Terrorist Screening Center's Screening Database (TSDB). EPMP also uses the TSA Performance and Results Information System (PARIS) for statistical information.

While dominated by statistical information, AIM, PMIS and PARIS maintain some PII on employees and members of the public.

Categories of PII Maintained in AIM: Employee information used for the management of operations (such as service information, pay band, supervisor, leave data, contact information, work schedules, uniform issuance, controlled property tracking); employee dependent names, dates of birth, and emergency contact information; customer service information such as complaints/compliments, lost and found item identifications, and damaged bags identification;

and; information relating to individuals involved in incidents at the facility (may include security incidents or non-security incidents such as slip and fall, theft, etc).

Categories of PII in PMIS: Individuals under special travel arrangments (such as diplomatic considerations or escorted travel); and individuals identified in the TSDB, as posing a threat to transportation or national security.

Categories of PII in PARIS: Individuals and witnesses involved in certain significant security incidents.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Pursuant to 49 USC § 114, TSA is responsible for security in all modes of transportation. TSA is also responsible for providing for the screening of all passengers and property. 49 U.S.C. § 44901. TSA has broad authority to receive, assess and distribute intelligence information related to transportation security, assess threats to transportation security, and serve as the primary liaison for transportation security to the intelligence and law enforcement communities. 49 U.S.C. § 114(f). TSA is also required to, on a day-to-day basis, manage and provide operational guidance to the field security resources, and enforce security-related regulations and requirements. 49 U.S.C. § 114(f).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) applies to the information?

Most information in EPMP does not involve PII. PII in EPMP subject to the Privacy Act fall within:

AIM: Correspondence and Matters Tracking, DHS/TSA 006, 75 FR 18863, April 13, 2010; Office of Personnel Management, General Personnel Records OPM/GOV'T-1, 71 FR 35356, June 19, 2006; and National Finance Center Payroll Personnel System, DHS/TSA 022, 71 FR 40530, July 17, 2006.

PMIS: Transportation Security Enforcement Record System (TSERS), DHS/TSA 001, 75 FR 28042, May 19, 2010; and Transportation Security Intelligence Service (TSIS) Operation Files, DHS/TSA 011, 75 FR 18867, April 13, 2010;

PARIS: Transportation Security Enforcement Record System (TSERS), DHS/TSA 001, 75 FR 28042, May 19, 2010;

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. The Performance Measurement Information System (PMIS) received a two-year Authority to Operate (ATO) on September 30, 2010. The Performance Information Management System (PIMS), which is a business tool used to manage data within EPMP, received a two-year ATO on March 31, 2010.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Some of the information in EPMP is covered by a NARA-approved record retention schedule. Data in PMIS concerning passenger, baggage and cargo screening statistical reports (e.g., passenger counts, number of incidents, abandoned property) is maintained for five years. PARIS records are maintained for three years.

TSA will seek NARA approval for record retention schedules covering the information in EPMP not currently covered by existing schedules. TSA will seek to retain AIM and PMIS data that currently has no approved schedule for up to five years. TSA will seek to retain employee dependent information for one year after the employee leaves TSA. Non-PII statistical data on such individuals is expected to be maintained in EPMP for 13 months for metrics purposes. Lost item and damaged baggage information will be retained for three years.

TSA will seek to retain data containing PII related to the movement of individuals with special travel arrangements for 30 days after the travel is completed. TSA will seek to retain information on individuals identified in the TSDB who pose a threat to transportation or national security for 30 years, to establish a database that is able to be queried on behalf of TSA for trends and other analysis.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The Paperwork Reduction Act of 1995 (44 U.S.C. § 3507(d)) requires that TSA consider the impact of paperwork and other information collection burdens imposed on the public. There is no current or new information collection requirements associated with the systems covered by this PIA.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

EPMP maintains a wide variety of non-PII data associated with management of security operations at airports. It also maintains a wide variety of information on TSA employees that is used to manage operations.

AIM:

For lost and found items, name and address will be collected for those items that are associated with an owner.

For damaged bags, passenger name and airline contact information will be collected.

Individuals who are dependents of TSA employees will have their name, date of birth, and emergency contact information maintained in EPMP.

When a complaint or compliment is submitted to TSA, name and contact information will be collected for the individual.

PMIS:

Name, date of birth, gender, passport information (if available), and flight information will be collected for individuals requiring special travel arrangements when traveling through an airport, and for passengers identified in the TSDB posing a threat to transportation or national security.

PARIS or AIM:

EPMP maintains the following PII on members of the public involved in an incident (security or non-security) at the transportation facility:

1. Name;
2. Driver's License number (if available;)
3. Passport number (if available;)
4. Physical description;
5. Date of birth;
6. Gender;
7. Address;
8. Contact information;

9. Military status (branch, traveling on orders);
10. Watchlist status; and
11. Results of any law enforcement checks for individuals involved in an incident at the facility.

2.2 What are the sources of the information and how is the information collected for the project?

EPMP is primarily a data management system using information from other TSA systems. The underlying TSA systems that use PII collect information either directly from the individual or from third parties, including law enforcement and intelligence agencies, or transportation facility operators, including PARIS.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

EPMP uses non-PII airline and flight information provided by a commercial source.

2.4 Discuss how accuracy of the data is ensured.

The accuracy of information input in EPMP is important to support the effective use of the program. Accuracy of the information in the underlying systems is derived by collecting the information from the individual where possible. The accuracy of lost and found information is confirmed with the individual before shipping any item to the individual. EPMP relies on the accuracy of the underlying systems for information from third parties, including law enforcement, intelligence, or transportation facility operators.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that PII collected for varied reasons (e.g., lost baggage, employee dependents, threats to transportation or national security) will be exposed to use for unrelated or unauthorized purposes.

Mitigation: This privacy risk is mitigated by limiting access in EPMP to authorized DHS personnel. EPMP users are assigned specific roles, which limits their use of the system, as well as the data elements to which they have access. Further, all data entry and report actions are logged with username, and users are trained on the appropriate safeguarding of PII and Sensitive Security Information (SSI) as part of their employment with TSA. In addition, every

modification to EPMP functionality passes through the TSA standard software development life cycle (SDLC) and is reviewed by TSA's Office of Information Technology (OIT).

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

EPMP is principally used to generate statistical information to manage TSA security operations at transportation facilities. Accordingly, the PII in the system is not used to determine substantive rights of individuals since those determinations are typically made in the systems that feed to EPMP. For example, EPMP uses PARIS data to generate a statistical picture on violations of TSA regulations, but EPMP users do not use PARIS data to pursue civil or criminal penalties for such violations. In addition to statistical reporting, EPMP allows TSA to conduct further use and reporting as follows:

AIM information:

- Employee information is used for the management of operations (such as service information, pay band, supervisor, leave data, contact information, work schedules, uniform issuance, controlled property tracking);

- Employee dependent information is used for Safe Haven and Continuity of Operations purposes in the event of natural disaster or other catastrophic event and for emergency contacts;

- Complaints/compliments, lost and found item identifications, and damaged bags identification are used to improve customer service, address complaints and recognize meritorious performance, and unite individuals with lost items;

- Information relating to individuals involved in incidents (security or non-security) at the facility is used for statistical purposes related to management of the transportation facility. For example, number of prohibited items at an airport over a time frame, even if not a basis for civil or criminal prosecution; number of slip and fall claims; etc..

PMIS information:

- Information relating to individuals under special travel arrangments (such as diplomatic considerations or escorted travel) is used for situational awareness and operational purposes associated with the movement of the individual;

- Individuals identified in the TSDB as posing a threat to transportation or national security information are used for situational awareness and operational purposes

PARIS information:

PARIS information on individuals involved in certain significant security incidents is used by EPMP to generate statistical data for risk management at transportation facilities. While PARIS is the system that supports the prosecution of violations of transportation security regulations by individuals and regulated entities, EPMP only uses the data to generate statistics.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. EPMP does not use technology to identify predictive patterns or anomalies.

3.3 Are there other components with assigned roles and responsibilities within the system?

No, although other agencies (such as the Terrorist Screening Center and TSA employees located at the FBI) may be granted view access to the portion of EPMP that contains information on individuals who pose or may pose a threat to transportation security.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that PII may be disclosed to individuals without authorization.

Mitigation: This privacy risk is mitigated by limiting access in EPMP to authorized DHS personnel with role-based access. In addition, information may be disclosed to non-DHS users in accordance with the Privacy Act, for information on individuals who pose, or may pose, a risk to transportation security. EPMP users are assigned specific roles limiting their use of the system and potentially limiting the data elements to which they have access. All data entry and report actions are logged with username, and users are trained on the appropriate safeguarding of PII and Sensitive Security Information (SSI) as part of their employment with TSA. Furthermore, every modification to EPMP functionality passes through the TSA-standard SDLC and is reviewed by TSA OIT to ensure that these controls remain in place.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

EPMP does not directly collect information; rather, it utilizes data received from TSA systems. Depending on the source system, TSA may provide notice of the collection of information. For example, individuals submitting complaints or compliments receive a notice that TSA is collecting the information they submit, but individuals in the TSDB will not. Likewise, individuals who have lost property will not get notice because TSA will have no one to give notice to before collecting the information. Similarly, where TSA discovers a damaged bag, it notifies the aircraft operator but may not have any means to notify the individual.

This PIA and the SORNs referenced in this document provide notice of the collection of the information covered in this PIA.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

None.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that the individual will not have prior or existing notice of the collection.

Mitigation: Mitigation measures for this risk include limiting access to the EPMP system to authorized users and for authorized purposes. PII contained within EPMP is collected through other TSA systems or applications and either collected directly from the individual, or from third parties, including law enforcement, intelligence or transportation facility operators. Individuals are provided notice of the initial TSA collection, except in the case of individuals who pose or may pose a threat to transportation or national security. TSA may receive information on individuals under special travel arrangements directly from the individual, their representatives, or other officials. PII collected from baggage tags or lost property identifiers is collected without notice but is presumably placed on those items by individuals with the intent that it be used to identify them. EPMP uses PII for purposes consistent with the initial collection.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

Some of the information in EPMP is covered by a NARA-approved record retention schedule. Data in PMIS concerning passenger, baggage and cargo screening statistical reports (e.g., passenger counts, number of incidents, abandoned property) is maintained five years. PARIS records are maintained for three years.

TSA will seek NARA approval for record retention schedules covering the information in EPMP not currently covered by existing schedules. TSA will seek to retain AIM and PMIS data that currently has no approved schedule for up to five years. TSA will seek to retain employee dependent information for one year after the employee leaves TSA. TSA will also seek to retain data containing PII related to the movement of individuals with special travel arrangements for 30 days after the travel is completed. However, TSA will seek to retain information on individuals identified in the TSDB who pose a threat to transportation or national security for 30 years, to establish a database that is able to be queried on behalf of the TSA for trends and other analysis. Non-PII statistical data on such individuals is expected to be maintained in EPMP for 13 months for metrics purposes. Lost item and damaged baggage information will be retained for three years.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that PII will be retained by TSA for longer than it is required or needed.

Mitigation: This risk is mitigated by the fact that retention of PII within EPMP is consistent with others systems holding the same or similar data. For example, the 30-year retention of information on individuals identified in the TSDB who pose a threat to transportation or national security is logged consistent with the NARA-approved 30-year watch log retention schedule. The retention of employee dependent information in EPMP for five years after termination of employment is consistent with the NARA-approved emergency preparedness records schedule. PII on individuals under special travel arrangements will only be retained for 30 days in order to permit reasonable time to discover and address issues that may have been associated with the travel. Lost item and damaged baggage information will be retained for three years consistent with the NARA-approved customer service records schedule.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Most EPMP information is not shared outside DHS. Users from the Terrorist Screening Center have read access to the portion of EPMP on individuals who pose or may pose a threat to transportation or national security. Information within EPMP may be shared with other agencies external to DHS in accordance with the Privacy Act of 1974. TSA will share damaged bag information with the airline carrying the bag.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Pursuant to routine use "I" in both TSERS and TSIS, TSA may share information with appropriate federal, state, tribal, local, foreign, or international agencies, regarding individuals who pose, or are suspected of posing, a risk to transportation or national security. This is compatible with the original collection because TSA is statutorily required to assess threats and make plans related to transportation or national security, and on a day-to-day basis manage and provide operational guidance to the field security resources, as well as enforce security-related regulations and requirements. Sharing damaged bag information with the airlines is permitted under routine use "S" in TSERS, which permits sharing with airlines when required for administrative purposes related to the effective and efficient administration of transportation security laws.

6.3 Does the project place limitations on re-dissemination?

EPMP does not place a limitation on re-dissemination.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Records of notifications outside of DHS will be maintained manually until an automated function can be developed and implemented.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk when PII is shared beyond DHS.

Mitigation: The risk associated with sharing information outside DHS is minimal since the external agencies typically already possess all or some of the information being sent in the notification and are trained on how to protect sensitive information. For example, PII on individuals who pose or may pose a threat to transportation or national security most often originates outside of TSA. It is only the information on the interaction with TSA that is new to those external agencies. PII associated with damaged baggage is also typically already held by the airline handling the baggage.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Individuals may request access to their data by contacting the TSA Headquarters Freedom of Information Action (FOIA) Officer, at FOIA Officer, Transportation Security Administration, Arlington, VA 20598-6020. Privacy Act exemptions have been asserted under 5 USC §§552a(j)(2), (k)(1), (k)(2), and (k)(5) for the systems of record under which EPMP operates.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals may have an opportunity to correct their data when it is being collected within the source systems; otherwise, they may submit a Privacy Act request as described in 7.1.

7.3 How does the project notify individuals about the procedures for correcting their information?

EPMP has no direct interaction with any individual and does not notify individuals about procedures to correct information. PII contained within EPMP is collected through other TSA systems or applications and either submitted directly by the individual, or by law enforcement officers when there is an incident involving law enforcement. In each instance, the individual is provided notice of the initial TSA collection and correction mechanisms, except that individuals identified in the TSDB who pose or may pose a threat to transportation or national security do not necessarily receive such notice. Individuals traveling under special arrangements do not have information to correct since they or their representatives or other officials provide information for their movement that is confirmed during the movement. PII collected from

baggage tags or lost property identifiers is collected without notice but is presumably placed on those items by individuals with the intent that it be used to identify them and that it is correct.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that redress options related to the EPMP systems are limited**.**

Mitigation: Redress limitations within EPMP are mitigated by the fact that EPMP does not make operational decisions on individuals. EPMP is principally a metrics system and provides a communications medium to the airport staff for notifications on movements of individuals under special travel arrangements, and individuals posing a risk to transportation or national security. With respect to passengers warranting additional screening because their prior conduct indicates a prudent and operational security basis to do so, DHS Traveler Redress Inquiry Program (TRIP) may be used to seek redress.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

All EPMP report access is tracked in a "statistics" project, and report access trends are reported on a weekly basis. In addition, report access is routinely analyzed and audited by the system owner and ISSO to ensure that reports are run by only the appropriate individuals. EPMP includes the ability to specifically identify – via a documentation wizard – all objects to which an individual or group has access. Finally, the system has over 30 roles into which users are grouped, and each role can be assigned access to only specific portions of the applications.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All users are required to complete courses covering SSI, Privacy, and information protection. In addition, system-specific training is provided to users in the proper and efficient use of the applications.

8.3 What procedures are in place to determine which users may access the information and how does the project determined who has access?

All access requests are submitted to the EPMP helpdesk in writing, and each access

request must be approved by an authorizing official. Users internal to DHS must have an official need for the information in the performance of their duties. Users external to DHS are limited to "read-only" access to information on individuals who pose or may pose a threat to transportation or national security in accordance with the Privacy Act. Users are grouped into roles according to job responsibility or "least privilege" requirements to complete their job function, and user permissions can be modified upon request. Certain users may have 'read-only' access while others may be permitted to make certain amendments or changes to the information. External storage or communication devices are not permitted to interact with the system; all access is conducted via web browser.

8.3 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All MOUs are reviewed by the program manager, component Privacy Officer, and counsel and then sent to DHS for formal review.

Responsible Officials

James Watts
Operational Process & Performance Metrics
Transportation Security Administration
Department of Homeland Security

Approval Signature

(Original signed copy on file with DHS Privacy Office)

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security