Privacy Impact Assessment
for the

TSA Enterprise Search Portal (ESP)

DHS/TSA/PIA-033

May 5, 2011

Contact Point
Jerry C. Booker
Office of Intelligence
Transportation Security Administration
703-601-3169

Reviewing Officials

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

Abstract

The Transportation Security Administration (TSA) is implementing a search capability to enable authorized users to search or discover[1] data held by separate databases within TSA. The search function will be known as the Enterprise Search Portal (ESP). TSA is conducting this Privacy Impact Assessment to assess privacy impacts associated with this capability to search across multiple databases. The systems being searched are covered by other PIAs or are otherwise compliant with the E-Government Act of 2002.

Overview

Pursuant to Section 114 of the Aviation and Transportation Security Act (ATSA) (Pub. L. 107-71, November 19, 2001, 115 Stat. 597), TSA is responsible for security in all modes of transportation, and is required to "receive, assess, and distribute intelligence information related to transportation security," as well as to "assess threats to transportation." Currently, authorized TSA employees perform independent searches of several databases held by TSA in order to perform security functions. Separate searches are inefficient and reduce the ability of analysts to understand relationships between incidents, individuals, locations, and threat items in incidents or intelligence that may have initially been collected and maintained by different offices within TSA.

ESP users are able to search any combination of databases using a natural language query as well as other parameters, such as airport code and incident type, and can delimit the search by date or range of dates. The system will return a set of results based on the search, and also provide the ability to display information in a "discovery mode." This will allow for a relationship to the data searched but is prompted by the system rather than by search terms selected by the user.

ESP will search across systems that have compatible purposes, and users will undergo an approval process prior to getting access to data from new systems. For initial operating capability, ESP will search across the Tactical Information Sharing System (TISS),[2] the Operations Center Incident Management System (OCIMS),[3] and the Performance and Results Information System (PARIS). Users from within the Office of Security Operations, Office of Law Enforcement, and Office of Intelligence who are approved access to these databases through ESP will use the system to assess threats and risks to transportation. In order to assess risks and threats to transportation from transportation sector workers who may have "insider" type access, TSA will add users from the Office of Transportation Threat Assessment and Credentialing

[1] The "discovery" capability permits the system to identify relationships between data that is prompted by the system (rather than a specific user search) based on a taxonomy of terms.
[2] See http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_tiss.pdf
[3] See http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_ocims_update.pdf

(TTAC), and the TTAC Crew Vetting Platform (CVP) as the TTAC database for ESP. This PIA will be updated if additional systems are added, or if ESP is used for new purposes.

For example, currently if TSA wishes to know whether an individual involved in an incident at an airport has previously been involved in an incident, TSA must perform independent queries across three different databases. To know whether the individual is part of a worker population that may have special access to transportation assets, additional databases would need to be checked. ESP permits a single query to search across multiple databases to get an understanding of whether the individual involved in an incident has been involved in prior incidents, or is part of a worker population with special access to transportation assets. The "discovery" mode might be used, for example, if an authorized user had a particular interest in a particular airport, or mode of attack. Searches could be run each day to provide updated visibility into the data coming into TSA without the user having to prompt a daily search.

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?

TSA is responsible for security in all modes of transportation. 49 U.S.C. §114(d). TSA is required to "receive, assess, and distribute intelligence information related to transportation security" as well as to "assess threats to transportation." 49 U.S.C. §114(f). ESP functions are directly related to TSA's statutory requirement to assess transportation security risks. ESP provides a search and discovery capability for information initially collected by other TSA systems.

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

The information within the ESP that is subject to the Privacy Act is covered by several SORNs, including Transportation Security Enforcement Record System (TSERS), DHS/TSA 001, 75 FR 28042, May 19, 2010; Transportation Security Threat Assessment System (TSTAS), DHS/TSA 002, 75 FR 28046, May 19, 2010; and Transportation Security Intelligence Service (TSIS) Operation Files, DHS/TSA 011, 75 FR 18867, April 13, 2010.

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

Yes.

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

Records from the underlying systems that are searched by ESP will be retained in accordance with schedules approved by NARA for those systems. TSA will seek to retain queries saved by users within the system in order to provide the capability to run the same query in the future. For example, a particular user's investigative interest in security breaches at a particular airport can be saved to run the search on a daily basis. TSA will seek approval from NARA to retain queries for five years. The results of these queries will be retained outside of ESP in accordance with records schedules that apply to the particular user. For example, users from the Office of Intelligence may retain query results in accordance with NARA approved records schedules that apply to that office (Routine and non-significant case files will be retained for 30 years; significant case files will be retained permanently; working files will be destroyed when no longer needed for operational purposes). Users from the Office of Law Enforcement may retain query results for up to 25 years for information input to TISS, while more routine query results may be retained for three years within OCIMS. Users from other offices will likewise retain query results pursuant to approved records schedules that apply to their offices.

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 TSA to consider the impact of paperwork and other information collection burdens imposed on the public. There is no current or new information collection requirement 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.

The ESP uses a wide variety of non-PII and PII data collected by TSA personnel and other law enforcement personnel associated with TSA's management of security operations at transportation venues and suspicious incidents. PII on members of the public may include such items as:

- Name;

- Drivers' License number (if available);
- Passport number (if available);
- Physical description;
- Date of birth;
- Gender;
- Address;
- Contact information;
- Military status (branch, traveling on orders);
- Watchlist status; and
- Results of law enforcement checks.

It also includes information associated with any incident initially collected by TSA, such as prohibited items, conduct, and witness information.

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

The ESP exists to perform a search by users or in discovery mode across multiple systems using information originally collected by other TSA systems. ESP does not collect information directly from individuals. The intent of the ESP is to provide greater efficiency and visibility into the data currently held by TSA in disparate databases.

ESP will search across the Tactical Information Sharing System (TISS),[4] the Operations Center Incident Management System (OCIMS),[5] the Performance and Results Information System (PARIS), and Crew Vetting Platform (CVP).[6]

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

No, ESP does not use information from commercial sources.

2.4 Discuss how accuracy of the data is ensured.

ESP relies on the accuracy of the existing databases across which it will search. The data is pulled directly from existing TSA data stores and is not modified once imported into the ESP platform. Any modifications to the underlying database will result in a corresponding modification to the record searched in ESP. Query results that are stored by the user will not be updated based on changes to the underlying database unless the user re-runs the query.

[4] See http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_tiss.pdf
[5] See http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_ocims_update.pdf
[6] See http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cvp.pdf

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that ESP will perform search functions that could previously only have been performed in separate searches within each individual database, allowing users more access to a larger amount of data.

Mitigation: The privacy risk is mitigated by limiting access to authorized users and logging user activity within ESP. As a practical matter, the identical search could have been performed by users of the individual systems and results shared with employees who needed the information in the performance of their duties. ESP provides a more efficient means for performing the individual searches, including the ability to discover information not prompted by a user search. ESP reduces the number of users that may have to perform the same search, thereby reducing the exposure of the data. ESP functions are directly related to TSA's statutory requirement to assess transportation security risks. Data is accurate and complete because ESP searches use data from the underlying databases and are updated as those underlying systems are updated.

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.

The ESP is used to search across existing databases to assess risk in transportation venues. For example, if an incident raises a concern about an individual, ESP can be used to determine whether there have been previous incidents involving the individual. In addition, ESP may also be used to determine whether the individual may have some form of "insider" access to a transportation facility as a TSA employee or employee within a transportation mode that is regulated by TSA. Similarly, if there is intelligence about threats to a particular location, ESP can be used to search for prior incidents at that location or involving particular threat items. Further, ESP may be used to evaluate trends and generate statistical information about indications of or actual threats, incidents types, and locations, and to provide informed analysis and information to TSA officials in the performance of their duties.

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, ESP can be used to identify historical trends and links, but does not use technology to predict individual behavior or patterns.

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

No.

3.4 <u>Privacy Impact Analysis</u>: Related to the Uses of Information

<u>Privacy Risk:</u> There is a risk of disclosure of PII to individuals without authorized access.

<u>Mitigation:</u> This risk is mitigated by limiting access to ESP to authorized TSA personnel with a need for the information in the performance of their duties consistent with the Privacy Act, 5 U.S.C. §552a(b)(1). Data entry and report actions are logged by username. Users are trained on the appropriate safeguarding of PII and Sensitive Security Information (SSI) as part of their employment with TSA. Disclosures of information are consistent with the published routine uses for each system from which data may be pulled.

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.

The ESP does not provide notice to individuals since it does not collect information directly from individuals. It provides a search capability across existing TSA databases.

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

There are no opportunities for individuals to consent to use, decline to provide information, or opt out of the ESP.

4.3 <u>Privacy Impact Analysis</u>: Related to Notice

<u>Privacy Risk:</u> There is a risk that ESP search results may contain PII, but the system search does not allow for prior notice or consent to its usage by individuals.

<u>Mitigation:</u> This risk is mitigated by the fact that PII accessed by ESP searches is maintained by other TSA systems. In general, the individual is provided notice of the initial TSA collection. However, individuals who pose or may pose a threat to transportation or national security do not receive individual notice, though public notice has been provided through publication of this PIA. ESP 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.

Records from the underlying systems that are searched by ESP will be retained in accordance with schedules approved by NARA for those systems. Because ESP provides a search and discovery capability on data held in other systems, ESP is periodically refreshed by the data from those systems and therefore the information in ESP necessarily matches additions and deletions to those systems.

TSA will seek to retain queries saved by users within the system in order to provide the capability to run the same query in the future. For example, a particular user's investigative interest in security breaches at a particular airport can be saved to run the search on a daily basis. TSA will seek approval from NARA to retain queries designated for retention by users for five years to provide for reasonable repetition of queries.

Query results will be retained outside of ESP in accordance with records schedules that apply to the particular records storage location used by the user. The records storage location will be determined by where the user stores their research. Typically, this will be on the individual computers where their working files are stored. One exception is TISS, as TISS users will store the information for their investigations in TISS.

As ESP merely provides a more efficient search and discovery capability for users who retain query results in investigative files, watchlogs, and briefing materials, the retention period is based on existing retention practices and investigative need and authority of each user. For example, users from the Office of Intelligence may retain query results in accordance with NARA approved records schedules that apply to that office (Routine and non-significant case files will be retained for 30 years; significant case files will be retained permanently; working files will be destroyed when no longer needed for operational purposes). Users from the Office of Law Enforcement may retain query results for 25 years for information input in TISS, while more routine query results may be retained for three years within OCIMS.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that ESP may result in retaining data longer than the underlying systems.

Mitigation: This is risk is mitigated by the fact that queries and query results will be maintained based on existing retention practices, determined by the investigative need and authority of each user. It is possible that a user's retention of a query result in a case file may be longer than the retention of data in the underlying system from which the data is taken. This risk is inherent in federal records retention where different parts of an agency may have differing needs for the information. Retention of query results relating to security threats is aligned with the purpose and mission of the agency, and permitting the underlying system to delete information when it is no longer needed by that system protects PII by reducing the proliferation of the data.

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.

ESP is a search capability across existing TSA databases. The existing TSA databases may share information in accordance with the Privacy Act. It is expected that while the majority of ESP functions will not involve sharing information outside of DHS, ESP may, in the course of normal operations, identify individuals who pose or may pose a threat to transportation or national security and that such information may be shared outside of DHS.

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

Each of the TSA systems for which ESP provides a search capability contains routine uses permitting the sharing of information with appropriate federal, state, tribal, local, foreign or international agency, regarding individuals who pose, or are suspected of posing, a risk to transportation or national security. This is compatible with the original collection of each underlying database because TSA is statutorily required to assess threats and make plans related to transportation or national security.

6.3 Does the project place limitations on re-dissemination?

No, ESP provides a search capability but otherwise relies on authorized users to appropriately handle the results of the query.

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

ESP only provides a search capability. Any disclosures outside of DHS will be manually recorded and maintained with the query result that led to the disclosure.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information will be disclosed beyond what would have been contemplated in the underlying systems.

Mitigation: The risk associated with ESP is mitigated by the fact that external disclosures are consistent with those already contemplated in the databases across which ESP can search. For example, if ESP reveals that an individual identified in an incident in the TISS system is the same individual identified in another incident in the OCIMS system, external disclosures will be consistent with disclosures permitted by both of those systems.

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. The source systems may, however, be exempt from access under the Privacy Act.

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. The source systems may, however, be exempt from the access and correction provisions of the Privacy Act and therefore access to such records may be restricted.

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

The ESP has no direct interaction with any individual and does not notify individuals about procedures to correct information. PII contained within ESP is collected through other TSA systems.

7.4 Privacy Impact Analysis: Related to Redress

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

Mitigation: The lack of redress options for ESP is mitigated by the fact that ESP is a search capability across existing TSA databases with existing redress processes. ESP does not change any of the underlying database records, and because it relies entirely on the underlying databases, it creates no new risk related to 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 ESP user access can be analyzed and audited by the system owner and Information System Security Officer to ensure that reports are run by only the appropriate individuals and for authorized purposes.

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

All users are required to complete TSA-mandated Online Learning Center (OLC) 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 determine who has access?

All access requests are submitted to the ESP core team in writing, with each access request being approved by an authorizing official. Users must have an official need for the information in the performance of their duties in each of the databases that ESP will search.

External storage or communication devices are not permitted to interact with the system. All access is conducted via Web browser.

8.4 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?

It is not expected that ESP will be used by external users, but MOUs are reviewed by the program manager, TSA Privacy Officer, and counsel and then sent to DHS for formal review. It is not anticipated that ESP will have new uses, but any such uses will be addressed in updates to this PIA.

Responsible Officials

Jerry Booker
Office of Intelligence
Transportation Security Administration
Department of Homeland Security

Approval Signature

(Original signed copy on file with the DHS Privacy Office)

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security