Privacy Impact Assessment
for the

Transportation Security Administration Performance and Results Information System (PARIS)

DHS/TSA/PIA-038

September 18, 2012

Contact Point
Russ Miller
Office of Security Operations Compliance
Transportation Security Administration
Russell.Miller@tsa.dhs.gov

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Transportation Security Administration (TSA) Performance and Results Information System (PARIS) is a database used for maintaining information associated with TSA's regulatory investigations, security incidents, and enforcement actions, as well as for recording the details of security incidents involving passenger and property screening. PARIS maintains personally identifiable information (PII) about individuals, including witnesses, involved in security incidents or regulatory enforcement activities. PARIS also creates and maintains a list of individuals who, based upon their involvement in security incidents of sufficient severity or frequency, are disqualified from receiving expedited screening for some period of time or permanently. The purpose of this Privacy Impact Assessment (PIA) is to inform the public of changes in the use of PARIS and any resulting impact to personal privacy.

Overview

PARIS is the primary security incident, as well as regulatory inspection and assessment reporting mechanism within TSA. PARIS is used to report security incidents at airport checkpoints that may violate laws or regulations promulgated under TSA's authority, such as passengers with firearms or other prohibited items, or Behavior Detection Officer referrals to law enforcement officers. PARIS also is used to record the results of TSA inspections conducted on aircraft operators, cargo, airports, and other facilities or operations within TSA's authority. These may include, for example, unlocked secured area access doors, or badge violations. Data recorded in PARIS is the source data for enforcement actions against individuals involved in security incidents, and for enforcement actions against individuals and entities as a result of regulatory inspections and assessments of transportation sector facilities and entities. PARIS data is also used to provide statistical and incident data for security management purposes.

PARIS data aid TSA efforts to ensure compliance with security regulations and requirements. TSA compliance efforts employ a progressive enforcement philosophy that applies more punitive enforcement action in response to repeated violations, failure of a regulated entity to take effective corrective action, flagrant violations, and violations that indicate chronic problems. Enforcement actions for security violations by individuals involve either Administrative Actions[1] or Civil Penalty Actions.[2]

[1] Administrative actions include Warning Notices, Letters of Correction, and Notices of Noncompliance. A Warning Notice recites available facts and information about the incident and indicates that the incident may have been a violation of transportation security requirements. A Letter of Correction confirms TSA's decision on whether a violation took place and states the necessary corrective actions the alleged violator has taken or agrees to take. A Notice of Noncompliance is issued only to public transportation agencies providing them with notice and opportunity to correct non-compliance issues. 49 C.F.R. § 1503.301.

[2] Some security incidents concerning individuals result in civil penalty action. A Notice of Violation (NOV) is used to initiate a civil penalty action when there is an absence of serious aggravating factors and where the proposed civil penalty is less than $5,000 against an individual who violated 49 C.F.R. § 1540.111. Civil Penalty Actions for violations that do not meet the criteria for an NOV are initiated by a Notice of Proposed Civil Penalty issued by the TSA Office of Chief Counsel. TSA has the authority to assess civil penalties up to $11,000 per violation against individuals. 49 C.F.R. § 1503.401. A third type of Civil Penalty Action is a Civil Penalty Letter. Civil Penalty Letters are issued in cases where the total civil penalty proposed exceeds TSA's statutory maximum. These enforcement actions are referred to the Department of Justice for prosecution of a civil action in a U.S. District Court.

PARIS data also are used in air traveler security screening decisions through the creation and management of a list of individuals who are disqualified from eligibility to participate in the TSA Pre✓™ program for expedited screening (the TSA Pre√™ Disqualification Protocol List). TSA Pre✓™ is a program under which TSA uses Known Traveler data from certain populations, such as U.S. Customs and Border Protection's (CBP) Trusted Traveler programs, as well as data regarding certain frequent flyers for U.S. airlines, to identify air travelers who are eligible for expedited security screening at the airport checkpoint.[3] Under TSA Pre✓™, however, individuals involved in security incidents of sufficient severity or frequency are disqualified from receiving expedited screening for some period of time or permanently. Disqualifying security incidents may involve violations at airports or onboard aircraft or in connection with air cargo, or bomb threats in any transportation mode. For example, a person who brings a firearm to a checkpoint may be ineligible to receive expedited screening for a year or more. PARIS provides the TSA Pre✓™ Disqualification Protocol List to the TSA Secure Flight program for issuance of an appropriate boarding pass printing instruction.[4] The TSA Pre✓™ Disqualification Protocol List is updated to reflect additions and deletions to the List, as appropriate.

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 U.S.C. § 114, TSA is responsible for security in all modes of transportation. TSA is also responsible for providing the screening of all airline passengers and their accessible property.[5] In addition, pursuant to section 4012(a) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA),[6] TSA implemented Secure Flight as its pre-flight watch list matching program. TSA has broad authority[7] to receive, assess, and distribute intelligence information related to transportation security, to assess threats to transportation security, and to serve as the primary liaison for transportation security to the intelligence and law enforcement communities. Furthermore, TSA has regulatory authority[8] to enforce security responsibilities of aviation employees and other persons. TSA is required, on a day-to-day basis, to manage and provide operational guidance to the TSA field security resources, and to enforce security-related regulations and requirements.[9]

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

Information will be maintained in accordance with the applicable SORN, DHS/TSA-001, Transportation Security Enforcement Record System (TSERS), 75 FR 28042 (May 19, 2010).

---

[3] Additional information on TSA Pre✓™ is available at www.tsa.gov/what_we_do/escreening.shtm.
[4] For further information on how this list will be used in the TSA Secure Flight program, please refer to the Secure Flight PIA and related updates. http://www.dhs.gov/files/publications/gc_1280763432440.shtm#17.
[5] 49 U.S.C. § 44901.
[6] Pub. L. 108-458, 118 Stat 3638, Dec. 17, 2005.
[7] 49 U.S.C. § 114(f).
[8] 49 C.F.R. § 1540.105.
[9] 49 U.S.C. § 114(f).

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

Yes. System Authority to Operate (ATO) was approved on April 30, 2012.

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

TSA is seeking NARA authorization to maintain records for a period of twenty-five years in order to maintain records for use in enforcement matters and litigation, and to provide statistics for trends analysis. With regard to the TSA Pre√™ Disqualification List, this list will be deleted or destroyed when superseded, in accordance with the approved NARA schedule.

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.

PARIS does not require an information collection under the Paperwork Reduction Act. Incident information is taken from facts and opinions taken from direct observation by TSA personnel and from law enforcement officials.

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.

PARIS collects and maintains information on members of the public involved in (as subjects or witnesses) security incidents at airports or other transportation facilities, as well as individuals involved in regulatory inspections at such facilities. It also contains information on TSA employees involved in such activities as part of PARIS operations management functions. Such information includes:

- Name;
- Driver's 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 any law enforcement checks for individuals involved in a security incident.

PARIS also manages a list of individuals who have been disqualified from eligibility to receive expedited screening through the TSA Pre✓™ program for a period of time, or permanently, based upon their involvement in violations of security regulations of sufficient severity or frequency.

PARIS also maintains a wide variety of non-PII data associated with management of security operations at inter-modal ports of operation, such as number of weapons found, number of persons manually screened, and regulatory violations.

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

TSA employees input data to PARIS pursuant to incident reporting directives. The information is collected by TSA inspectors, investigators, supervisors, managers, or other TSA transportation security personnel by direct interaction with regulated transportation sector workers, law enforcement, and the public.

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

PARIS does not use information from commercial sources or publically available data.

2.4 Discuss how accuracy of the data is ensured.

The accuracy of information input into PARIS is important to support the effective use of the program. Accuracy of the information is maintained by collecting the information directly from the individual where possible. PARIS relies on the accuracy of the information entered by inspectors, investigators, supervisors, managers, and other TSA transportation security personnel. Additionally, PARIS has built in checks and balances to ensure accurate and timely entry of data. These checks and balances entail multi-level reviews and verification of the data.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There may be a risk of inaccurate information when it is collected from someone other than the individual.

Mitigation: PARIS may include information initially provided by an informant or other witness to the violation. The risk is mitigated by fully investigating the information before enforcement action is

taken. Enforcement action may be an adversarial process in which the accuracy of the information is tested.

Privacy Risk: There may be a risk of over-collection of information.

Mitigation: The risk is mitigated by limiting the functions of the system to security enforcement and management. There is no practical purpose to collecting information irrelevant to the underlying incident.

Privacy Risk: There may be a risk that PARIS maintains erroneous information about individuals**.**

Mitigation: The privacy risk is mitigated by collecting information from the individual involved and by emphasizing the importance of accurate data collection within the PARIS system. Enforcement actions based on PARIS data are administrative, civil, and criminal matters subject to great scrutiny. Redress options are provided by the TSA to correct inaccurate PARIS data.

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.

PARIS is a security incident and regulatory inspection and assessment reporting mechanism within TSA. It is the source of data for enforcement actions against individuals involved in security incidents or as a result of regulatory inspections and assessments of transportation sector facilities and entities. It is also used for security management purposes to provide statistical and incident data to TSA management.

PARIS collects information about incidents that occur within the transportation sector for use in enforcement proceedings against individuals and regulated entities, and for use in statistical trends analysis. It is also used to document results of inspections on transportation facilities and providers. For example, a facility inspection may reveal that an access door is unsecured in violation of a TSA regulation. The violation may be pursued in an enforcement proceeding seeking a civil penalty from the facility operator. The same information may be used statistically to identify whether the operator has a history of similar violations, or whether there is a similar issue across other facilities that may need to be addressed through greater inspection or outreach.

PARIS also uses the information on security incidents to generate and manage a list of individuals who are disqualified from eligibility to receive expedited screening through participation in the TSA Pre✓™ program. The TSA Pre√™ Disqualification Protocol List will be used by the TSA Secure Flight program for matching against passengers' and certain non-travelers' Secure Flight Passenger Data (SFPD)[10] to issue an appropriate boarding pass printing instruction to aircraft operators.

[10] SFPD consists of name, gender, date of birth, passport information (if available), redress number (if available), Known Traveler number (if available), reservation control number, record sequence number, record type, passenger update indicator, traveler reference number, and itinerary information.

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. PARIS 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, there are no other components with assigned roles or responsibilities within PARIS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

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.

PARIS collects information from individuals involved in an incident either as subjects, witnesses, or investigators. The initial information collection is typically open and obvious because the information is collected from the individual involved or under circumstances in which the individual has knowledge of the collection. This PIA and the applicable SORN[11] also 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?

There are no opportunities to consent to uses or opt out due to the law enforcement purpose of this system. Individuals may decline to provide information during an investigation but may be charged with interfering with the investigation.

4.3 Privacy Impact Analysis: Related to Notice

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

Mitigation: PII contained within PARIS is typically collected directly from the individual, or

[11] DHS/TSA-001, Transportation Security Enforcement Record System (TSERS), 75 FR 28042 (May 19, 2010).

from law enforcement officers, and TSA personnel who have collected the information directly from the individual. TSA provides notice on its website that individuals involved in security incidents may be disqualified from participation in TSA Pre✓™.

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.

TSA is currently seeking authorization to maintain PARIS records on security incidents, investigations, and assessments for a period of twenty-five years. The retention schedule is intended to permit use of PARIS data in enforcement matters and litigation, and to provide statistics for trends analysis. The current TSA Pre✓™ Disqualification Protocol List will be retained to reflect the addition and deletion of individuals as the list is superseded.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There may be a risk that PII will be retained by TSA for longer than it is required or needed to fulfill its statutory and regulatory missions.

Mitigation: This risk is mitigated by the fact that retention of PII within PARIS is consistent with other systems, such as the Tactical Information Sharing System (TISS) holding the same or similar data within TSA. Incident information is relevant to the identification of repeat offenders over what may be many years of travel, and for analysis of security trends over time.

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.

As part of normal operations, PARIS does not share information outside DHS. Information within PARIS may be shared with other agencies external to DHS in accordance with the Privacy Act of 1974. Such information, for example, may include information responsive to Congressional inquiries or U.S. Government Accountability Office (GAO) investigations.

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

Routine use "D" in DHS/TSA-001 TSERS permits sharing with any agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary or relevant to such audit or oversight function. Additional routine uses permit sharing with other entities.

6.3 Does the project place limitations on re-dissemination?

PARIS does not place a limitation on re-dissemination. Incident information may be Sensitive Security Information (SSI) pursuant to 49 U.S.C. § 114(r), and re-dissemination is limited by the SSI regulation, 49 C.F.R. Part 1520.

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

Records of disclosure outside of DHS are not a normal part of PARIS operations, but are maintained by recording disclosures manually in the individual record.

6.5 Privacy Impact Analysis: Related to Information Sharing

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

Mitigation: The risk associated with sharing information outside DHS is not a normal part of PARIS operations, and is further mitigated by sharing only as permitted by the Privacy Act of 1974. In addition, all TSA employees and contractors are required to take annual privacy training.

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?

Pursuant to the Privacy Act, individuals may request access to their data by contacting the TSA Freedom of Information Act (FOIA) Office, at Transportation Security Administration, TSA-20, 601 South 12th Street, Arlington, VA 20598-6020. Access may be limited pursuant to exemptions asserted under 5 U.S.C. §§ 552a(j)(2), (k)(1), (k)(2), and (k)(5) for the systems of record under which PARIS 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 initially collected during the investigation into the violation, for example, if the investigator or law enforcement officer requests confirmation of the facts; otherwise, they may challenge the underlying offense or penalty during the enforcement process in writing, or at a civil or criminal hearing. They may also submit a Privacy Act request as described in section 7.1. Individuals who have been disqualified from eligibility to receive expedited screening through participation in the TSA Pre✓™ program have an opportunity to correct or challenge the underlying disqualification offense during the enforcement proceeding.

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

PARIS does not interact with the individual whose information is collected by TSA or law enforcement during the investigation of a security incident, or regulatory inspection or assessment. Individuals disqualified from eligibility to receive expedited screening through participation in the TSA Pre✓™ program may seek redress through DHS TRIP and will be advised that if they were the subject of an enforcement action they should follow-up with the government enforcement contact such as the Transportation Security Investigator, to correct information. In addition, this PIA provides notice about procedures for correcting information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There may be a risk that individuals cannot obtain redress.

Mitigation: The risk is mitigated by above referenced measures which permit an individual to challenge the enforcement action.

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 PARIS access is recorded and routinely analyzed and audited by the System Owner (SO) and Information Systems Security Officer (ISSO) to ensure that only authorized personnel are accessing and utilizing the system. PARIS includes the ability to specifically identify all portions of the system to which an individual or group has access. Finally, the system has over 42 roles into which users are grouped, and each role has restricted access to only specific portions of the system.

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

All TSA employees and contractors are required to take annual privacy training.

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 PARIS resource center in writing after screening and approval by the Federal Security Director or approved staff representative. 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 are grouped into roles according to job responsibility, and user permissions can be modified upon request.

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?

PARIS primarily serves functions within TSA; therefore, there are no information sharing agreements or MOUs. All requests for new uses and access would be reviewed by the SO, ISSO, program manager, the component Privacy Officer, and counsel and then sent to DHS for formal review.

Responsible Officials

Frederick P Falcone
Office of Security Operations, Compliance
Transportation Security Administration
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security