**Privacy Impact Assessment Update
for the**

TSA Encounter Analysis Branch
(formerly Trends & Patterns Branch)

DHS/TSA/PIA-039(a)

October 12, 2017

Contact Point
Matthew Tracey
Encounter Analysis Branch
Office of Intelligence & Analysis
Transportation Security Administration
Matthew.Tracey@tsa.dhs.gov

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Transportation Security Administration (TSA) Office of Intelligence and Analysis (OIA), Encounter Analysis Branch (EAB) (formerly the Trends and Patterns Branch), seeks to improve TSA's ability to identify potential risks to transportation security by discovering and analyzing previously unknown links or patterns among individuals who undergo a TSA security threat assessment (STA), aviation passengers identified as a match to a watch list, and passengers who do not present acceptable identification documents to access the sterile area of an airport whose identity is unverified. TSA is updating the Privacy Impact Assessment (PIA) to reflect operational changes to the program.

Overview

TSA performs security threat assessments on workers within a variety of transportation sectors pursuant to its authorities under the Aviation and Transportation Security Act, 49 U.S.C. § 114. In general, TSA uses biographic and, when applicable, biometric information to perform security threat assessments on transportation sector workers by matching against Federal Government databases in order to identify potential risks to transportation security. Under the Secure Flight program,[1] TSA seeks to identify and prevent known or suspected terrorists or other individuals from gaining access to airports and airplanes when they may jeopardize the lives of passengers and others, by comparing passenger and non-traveler information to the No Fly List and Selectee List components of the Terrorist Screening Center Database (TSDB) and, when warranted by security considerations, other watch lists maintained by TSA or other federal agencies. Further, when passengers fail to present acceptable identification documents to enter the sterile area of an airport, TSA works with the individual to attempt to verify his or her identity to allow him or her to enter.

The TSA EAB seeks to improve TSA's ability to identify potential risks to transportation security by searching for, discovering, and analyzing previously unknown links, trends, or patterns among transportation sector workers and covered airline passengers. For example, the EAB may identify that an applicant for a transportation credential shared an address with an individual in the TSDB. Similarly, the EAB may identify that an individual failing to present acceptable identification for a flight is scheduled to fly with one or more individuals in the TSDB. EAB analysts may determine that further investigation or an operational response is warranted, produce intelligence reports on travel by known or suspected terrorists (KST), nominate an individual for inclusion in the TSDB, or enhance existing records within federal terrorism databases.

---

[1] For more information about the Secure Flight program, please see DHS/TSA/PIA-018 TSA Secure Flight Program available at https://www.dhs.gov/privacy, and DHS/TSA-019 Secure Flight Records, 80 FR 233 (January 5, 2015).

Reason for the PIA Update

TSA is updating this PIA to reflect that the EAB prepares a variety of reports, including a daily report for TSA executive leadership, Intelligence Information Reports, and 72-hour lookout reports for KST travel. Additionally, EAB prepares nominations to the TSDB based on associations and linkages that it discovers, and prepares record enhancements to existing records in federal terrorism databases. This update also reflects that the EAB has been granted access to the Secure Flight User Interface in order to view information on confirmed KST travel or to invalidate a reported match to a KST.

Privacy Impact Analysis

Authorities and Other Requirements

No changes.

Characterization of the Information

The EAB has been granted access to the Secure Flight User Interface[2] as a source of information on KST travel. This change is consistent with the EAB mission and assists in improving accuracy in reporting on KST travel, including instances in which EAB research indicates that the system match to a KST is incorrect.

Uses of the Information

EAB prepares a variety of reports, including a daily report for TSA executive leadership, Intelligence Information Reports, and 72-hour lookout reports for KST travel. These reports are used to provide leadership and security operations elements with situational awareness on potential KST movement within TSA systems. Additionally, EAB prepares nominations to the TSDB based on associations and linkages that it discovers, and prepares record enhancements to existing records in federal terrorism databases. For example, when a KST has applied for a transportation credential, the fact of the application and application information will be shared with the Terrorist Screening Center (TSC).

Notice

No changes.

---

[2] The Secure Flight User Interface only provides name, date of birth, and flight information, which is already listed as data elements in Section 2.1 of the original PIA. The Secure Flight User Interface is just a new data system that provides the information directly. The original PIA, DHS/TSA/PIA-039 Office of Intelligence & Analysis Trends and Patterns Branch (TPB), is available at https://www.dhs.gov/privacy.

Data Retention by the project

Intelligence reports and assessments to inform senior audiences and other transportation stakeholders of threats to civil aviation and other modes of transportation are retained until obsolescent or no longer needed (N1-560-04-12, Item 4b).

Information Sharing

The EAB may discover previously unknown links between transportation sector workers and KSTs. Such linkages may be reported to the TSC or other federal agencies, and may be used within TSA during the credentialing process. In addition, the EAB may nominate individuals to terrorism databases when appropriate.

Privacy Risk: There is a risk that EAB will draw linkages that are erroneous.

Mitigation: The risk is partially mitigated. While the vast majority of EAB reporting is based on flight information that is accurate, it is possible that an inaccurate linkage might be made within the population of transportation sector workers, such as a shared address with a KST. Such a linkage is not the sole factor in making a determination about the individual, but may be sufficient to initiate a deeper review by TSA.

Redress

No changes.

Auditing and Accountability

Use of the Secure Flight User Interface by the EAB is monitored and audited.

Responsible Officials

Matthew Tracey
Director (A), Vetting Analysis Division
Office of Intelligence and Analysis
Transportation Security Administration
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security