Privacy Impact Assessment Update
for the

TSA Encounter Analysis Branch
DHS/TSA/PIA-039(b)

July 2, 2019

Contact Point
Matthew Tracey
Encounter Analysis Branch
Intelligence & Analysis
Transportation Security Administration
Matthew.Tracey@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) Office of Intelligence and Analysis (I&A), Encounter Analysis Branch (EAB) seeks to improve TSA's ability to identify potential risks to transportation security. Initial efforts by the EAB involved discovering and analyzing previously unknown links or patterns among individuals who undergo a TSA security threat assessment (STA), passengers identified as a match to a government watch list, and passengers who do not present acceptable identification documents to access the sterile area of an airport whose identity cannot be verified through the identity verification process. TSA is updating the EAB Privacy Impact Assessment (PIA) to reflect operational changes to the program to include new investigative steps that may be taken in performing security threat assessment reviews on transportation sector workers and TSA Pre✓® participants.

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 individuals for appropriate screening or denial of boarding based on risk. TSA compares passenger and non-traveler information (for example, persons who are not flying but who are seeking access to the sterile area of an airport) to the No Fly 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 individuals 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 by contacting TSA's National Transportation Vetting Center (NTVC) so the individual can answer knowledge-based questions to sufficiently establish his or her identity.

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 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

---

[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).

TSA's encounters with known or suspected terrorists (KST), nominate an individual for inclusion in the TSDB, or enhance existing records within federal terrorism databases.

Reason for the PIA Update

TSA is updating this PIA to reflect the transfer within TSA of functional responsibilities relating to security threat assessment reviews on transportation sector workers and TSA Pre✓® participants to the EAB as a result of organizational changes, as well as new investigative steps involving reviews of open source information (including publicly available social media) being taken in performing security threat assessment reviews.

Privacy Impact Analysis

Authorities and Other Requirements

No changes.

Characterization of the Information

TSA performs security threat assessments on transportation sector workers across a wide variety of transportation modes and on individuals who have applied for or are already enrolled in TSA Pre✓®. As part of these assessments, EAB will provide input to the TSA Security Threat Assessment Board that makes recommendations to TSA leadership regarding the status of credentials of individuals for whom derogatory information has been identified. In addition, when TSA has identified derogatory information that does not clearly support denial or revocation of a credential or other authorized access to transportation but warrants further investigation, the EAB may review open source information, including publicly available social media, to ascertain whether there is information that may have a bearing on TSA's determination. TSA review of social media is conducted pursuant to DHS Management Directive 110-01, *Privacy Policy for Operational Use of Social Media.*[2]

Privacy Risk: Information collected from social media might be inaccurate and be used to affect the individual.

Mitigation: The risk is mitigated. TSA fully recognizes the importance of the investigation on the individual's livelihood or other travel privileges. Social media information is never the sole basis for TSA's determination. Social media may be used in concert with analysis of other information and after TSA determines an additional review is appropriate into whether a particular applicant should be denied a credential or have a credential revoked. In addition, TSA considers the source of the social media, apparent intent, severity of the content, credibility, context, and age of the postings, as well as exculpatory information, in making its assessment. TSA also takes steps to ensure that information collected from social media is accurately attributed

---

[2] DHS Management Directive 110-01, Privacy Policy for Operational Use of Social Media, *available at* https://www.dhs.gov/privacy.

to the individual seeking or holding a credential prior to considering this information as part of the individual's security threat assessment.

Uses of the Information

Information and analysis collected through social media or publicly available information about transportation sector workers and TSA Pre✓® participants will be used to assist TSA in making its determination to deny or revoke a credential or other authorization. The information may also be used to nominate transportation sector workers or TSA Pre✓® participants for inclusion in the TSDB, or enhance existing records within federal terrorism databases.

Notice

No changes.

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

No changes.

Redress

No changes.

Auditing and Accountability

No changes.

Responsible Officials

Matthew Tracey
Branch Manager (A), Encounter Analysis Branch
Office of Intelligence and Analysis
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