Privacy Impact Assessment Update
for the

TSA Operations Center Incident Management System

DHS/TSA/PIA-029(a)

August 25, 2015

Contact Point
John Bogers
System Owner
Transportation Security Operations Center
Transportation Security Administration
TSA-ocims@tsa.dhs.gov

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Transportation Security Administration (TSA) Transportation Security Operations Center (TSOC) serves as TSA's coordination center for transportation security incidents and operations. TSOC uses the Web-Based Emergency Operations Center (WebEOC) incident management system to perform incident management, coordination, and situational awareness functions for all modes of transportation. The system maintains information including personally identifiable information (PII) in connection with its operations. The system also collects and compiles reports from federal, state, local, tribal, foreign, and international sources and private sector security officials on incidents related to threats to transportation or national security. TSA is updating this Privacy Impact Assessment (PIA), last published on July 12, 2010, to reflect that the system receives information about individuals on watchlists and their co-travelers; logs Amber Alerts[1] and disseminates them to the field; collects open-source information relating to transportation security or operations matters; and collects PII related to other incidents reported to TSA including significant public health-related risks to the traveling public and certain TSA employee information.

Overview

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.[2] The Transportation Security Operations Center (TSOC) correlates and fuses real-time intelligence and operational information across all modes of transportation, and coordinates within DHS and with other federal, state, and local homeland security agencies for prevention of, and response to, transportation security-related incidents. TSA uses the Web-Based Emergency Operations Center (WebEOC) to store real-time information from federal, state, local, tribal, foreign, and international sources and private sector security officials to assist in performing transportation security functions. WebEOC stores information on individuals and witnesses involved in security incidents including: 1) individuals who violate or are suspected of violating transportation security laws, regulations, policies, or procedures; 2) individuals whose behavior or suspicious activity results in referrals to a Behavior Detection Officer or Law Enforcement Officer; and 3) individuals whose identity must be verified or checked against federal watch lists, including individuals who fail to show acceptable identification documents to compare to boarding documents and law enforcement officials who seek to fly armed.

---

[1] The AMBER Alert™ Program is a voluntary partnership between law-enforcement agencies, broadcasters, transportation agencies, and the wireless industry, to activate an urgent bulletin in the most serious child-abduction cases.

[2] 49 U.S.C. §114(f).

Reason for the PIA Update

TSA is updating this PIA, last published July 12, 2010, to reflect that TSA's Secure Flight System sends information to WebEOC regarding individuals who are a match to the Terrorist Screening Center's Terrorist Screening Database (TSDB) and their co-travelers, individuals on the Center for Disease Control's (CDC) Do Not Board list, and individuals who appear to be using lost or stolen travel documents for air travel. WebEOC stores information on known or suspected terrorists (KST) for TSA operational purposes including notifying field personnel of expected travel, and logs Amber Alerts to track the status of alerts issued to the field. WebEOC stores PII related to other matters reported to TSA, such as significant public health-related events posing risks to the traveling public.

WebEOC stores open-source information[3] related to transportation security matters for enhancing situational awareness and operational purposes. TSA monitors public open-source information, including social media, to gain situational awareness on events impacting transportation security or operations. It may use the information to assist in assessing threats and planning or managing an operational response. For example, a social media posting regarding the location a tornado touched down may assist with assessing impacts to transportation facilities or to the TSA workforce. Searches are performed based on keywords and concepts in reporting guidance that has been reviewed for privacy and civil liberties concerns. Search terms may be modified on occasion to reflect emerging or temporary threats.

WebEOC also stores TSA employee and contractor PII associated with such matters as medical evacuations, workplace violence, controlled property such as lost badges, continuity of operations (COOP) activities and exercises, and national or local emergencies.

PII is stored in separate modules within WebEOC based upon the type of information. For example, TSA employee PII may be stored in COOP, Critical Incident Management, or Federal Security Director Local Log modules; open-source information is stored in the Transportation Suspicious Incident Reports module. Access to each module is restricted at the user level to individuals with a need to know the information in the performance of their duties.

Privacy Impact Analysis

Authorities and Other Requirements

No changes.

[3] Open source information refers to a broad array of information and sources that are generally available, including information obtained from the Internet and media (e.g., newspapers, social media sites, radio, television), professional and academic records (e.g., papers, conferences, professional associations), and public data (e.g., government reports, public records, demographics, hearings, speeches).

Characterization of the Information

In addition to the information previously identified in prior PIAs, WebEOC collects and stores Secure Flight Passenger Data (SFPD)[4] regarding individuals who are a match to the TSDB and their co-travelers, individuals on the CDC's Do Not Board list, individuals who appear to be using lost or stolen travel documents for air travel[5], KST information, and PII related to matters reported to TSA, including significant public health-related risks to the traveling public.

To enhance situational awareness, assess threats, and assist with planning or managing an operational response, TSA may collect open-source information related to transportation security matters. Open-source information may include publicly available information or postings on social media sites regarding threats to transportation or national security, or simply matters potentially impacting TSA operations. Social media may also be a source of initial notification for transportation security or operations events. Open-source collection is accomplished through the use of search terms that have been reviewed for privacy and civil liberties impacts. TSA respects individual privacy settings when conducting open-source collection. Open-source information is assessed or corroborated prior to operational response.

Finally, WebEOC stores PII of TSA personnel reported to TSOC, such as medical evacuations, internal investigations, workplace violence, and lost badges. WebEOC will also store work status and contact information reported to TSOC by employees and managers during continuity of operations (COOP) activities, exercises, and national or local emergencies.

Privacy Risk: There is a risk of over-collection associated with the expansion of information collected by the system, including over-collection of open source information.

Mitigation: The risk is mitigated by only collecting information related to the TSOC mission as the coordination center for transportation security incidents and operations. Much of the information is already collected by TSA elsewhere and does not represent an expansion so much as centralizing existing information for coordination purposes. Open source information, including information collected from social media, is limited to transportation mission-related information that is available to the general public.

[4] 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. For more information on the Secure Flight program and SFPD, see DHS/TSA/PIA-018 Secure Flight Program and its associated updates, available at www.dhs.gov/privacy.
[5] TSA checks passenger reservation data including passport information against watch lists of lost and stolen travel documents, including international passports. For additional information, please see DHS/TSA/PIA-018(g) Secure Flight Program PIA (December 8, 2014), available at www.dhs.gov/privacy.

Uses of the Information

The information collected within WebEOC continues to be used for incident management, coordination, and situational awareness purposes. WebEOC will store TSA employee and contractor information to manage certain internal operations, such as medical evacuation, workplace violence, and lost badge reporting. TSA will also use the collected employee and contractor information for COOP activities and exercises and national or local emergencies.

Privacy Risk: There is a privacy risk of inappropriate use of the additional employee and contractor information to WebEOC storage.

Mitigation: The risk is mitigated by integrating administrative, technical, and physical security controls that protect PII against unauthorized disclosure. System users and managers receive privacy training. For log entries, incidents or reports are entered in real-time and the latest entry updates the entry.

Notice

Airline passengers receive notice that their information is submitted to TSA through Secure Flight; accordingly KST, co-traveler, CDC Do Not Board, public health threat, and individuals using lost/stolen travel documents receive notice.

TSA does not provide notice to individuals on the Amber Alert list, or to individuals identified in open-source information, except to the extent this PIA acts as notice.

Privacy Risk: There is a privacy risk that individuals who post PII on open source venues will not receive notice that TSA may collect their information.

Mitigation: The risk is mitigated by the fact that the information is taken from open sources that are available to the general public and typically posted by the individual. TSA respects privacy settings and only collects information that is available to the general public. PII is stripped from open-source reporting when it is not relevant to the event. For example, a social media posting that there is a fight on a plane does not require the PII of the individual poster. Information learned from open-sources is corroborated or evaluated for credibility prior to operational response.

Data Retention by the Project

TSA updated its retention schedule for WebEOC records from three years to ten years. TSA extended the retention period for these records to facilitate the review of incidents for trends over an extended time period. Maintaining information beyond three years also permits TSA to conduct queries to identify repeat offenders related to transportation or national security incidents.

Information Sharing

TSA shares information with CBP regarding individuals who are a match or a potential match to the TSDB and their co-travelers, individuals on the CDC Do Not Board list, individuals who appear to be using lost or stolen travel documents for air travel, and on significant public health-related matters or risks to the traveling public.

There are no new privacy risks as a result of this update. Expanding the categories of information shared with CBP does not create a new privacy risk because the types of information are similar to those previously shared.

Redress

No changes.

Auditing and Accountability

No changes.

Responsible Official

John Bogers
System Owner
Transportation Security Operations Center
Transportation Security Administration

Approval Signature

Original signed PIA on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security