Privacy Impact Assessment

for the

TSA Operations Center Information Management System

DHS Reference No. DHS/TSA/PIA-029(b)

December 5, 2022

Homeland Security

Abstract

The Transportation Security Administration (TSA) Transportation Security Operations Center (TSOC) serves as TSA's coordination center for transportation security incidents and operations. The Transportation Security Operations Center 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. WebEOC maintains information including personally identifiable information (PII). 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 to reflect the addition of several new collections of personally identifiable information, detailed below.

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. The Transportation Security Operations Center correlates and fuses real-time intelligence and operational information across all modes of transportation, and coordinates within the Department of Homeland Security (DHS) and with other federal, state, and local homeland security agencies for prevention of, and response to, transportation security-related incidents. TSA uses WebEOC to store real-time information from federal, state, local, tribal, and international sources, and private sector security officials to assist in performing transportation security functions.

WebEOC maintains boards (i.e., a community page within the WebEOC) that store information on a variety of matters including: information about individuals: (1) who violate, or are suspected of violating, transportation security laws, regulations, policies, or procedures; (2) whose behavior or suspicious activity become the subject of investigations or referrals to law enforcements; (3) whose identity must be verified or checked against federal watch lists, including individuals who fail to show acceptable identification documents; (4) who are verified law enforcement officials seeking to fly armed; (5) who match to the Terrorist Screening Center's Terrorist Screening Database (TSDB) and their co-travelers; (6) who are on the Center for Disease Control's (CDC) Do Not Board list; (7) who appear to be using lost or stolen travel documents; (8) who are on Special Mission Coverage (SMC) flights; and (9) who are TSA employees, contractors. WebEOC also includes personally identifiable information associated with: airline operations, medical evacuations, workplace violence, loss of controlled property such as badges, airspace violations, Special Mission Coverage,[1] personnel deployments, Visible Intermodal

[1] Flights with watch-listed Known or Suspected Terrorists (KSTs) or other high-risk travelers as a means of mitigating any potential threat posed by that individual.

Prevention and Response (VIPR) operations, Continuity of Operations (COOP) activities and exercises, and national or local emergencies.

Reason for the PIA Update

This update reflects the addition of Silent Partner/Quiet Skies (SP/QS) passenger information to the existing board which adds information about individuals on watch lists and information about their co-travelers. The Silent Partner/Quiet Skies program uses rules based on current intelligence as part of the Secure Flight vetting process to generate a temporary watch list of passengers selected for enhanced screening.[2] The TSA Federal Air Marshal Service (FAMS) also uses Silent Partner/Quiet Skies data as part of its flight coverage assessments.

This Privacy Impact Assessment update also reflects the addition of several new boards within WebEOC:

- A board to track requests from external agencies for Secure Flight passenger data pursuant to the Privacy Act.[3] This will improve management and administration of such requests;
- Transition to WebEOC of the TSA Workplace Violence Prevention Program[4] database regarding individuals involved in incidents of actual or alleged workplace violence, including those identified as confirmed or suspected aggressors, victims, or witnesses;
- Transition to WebEOC of the TSA Airline Operators database of air carrier contacts to assist TSA National Transportation Vetting Center (NTVC) operations with air carriers;[5]
- A board for National Capital Region Coordination Center (NCRCC) Airspace Authorizations/Waivers to coordinate, document, and maintain situational awareness of airspace authorizations/waivers within the National Capital Region (NCR);[6] and

[2] The rules are based on aggregated travel data, intelligence, and trend analysis of the intelligence and suspicious activity. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR SECURE FLIGHT, DHS/TSA/PIA-018 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

[3] Under 5 U.S.C. § 552a(b)(7) or as otherwise permitted under the Privacy Act.

[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR WORKPLACE VIOLENCE PREVENTION PROGRAM, DHS/TSA/PIA-027, *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

[5] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR GENERAL CONTACT LISTS, DHS/ALL/PIA-006, *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

[6] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR AIRSPACE WAIVER AND FLIGHT AUTHORIZATIONS FOR CERTAIN AVIATION OPERATIONS, DHS/TSA/PIA-003, *available at* https://www.dhs.gov/publication/airspace-waiver-and-flight-certain-aviation-operations-including-dca.

- A board for National Capital Region Coordination Center Uncrewed Aviation Systems (UAS) activity to coordinate, document, and maintain situational awareness of uncrewed aircraft authorizations/waivers and incidents within the National Capital Region.[7]

Privacy Impact Analysis

Authorities and Other Requirements

There have been no changes to the legal authorities.[8] 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.[9] Privacy Act System of Records Notice coverage for these records is provided by:

- DHS/TSA-001 Transportation Security Enforcement Records System;[10]
- DHS/TSA-002 Transportation Security Threat Assessment System;[11]
- DHS/TSA-011 Transportation Security Intelligence Services Operations Files;[12]
- DHS/TSA-019 Secure Flight Record; [13] and
- DHS/TSA-023 Workplace Violence Prevention Program.[14]

[7] *See* U.S. DEPARTMENT OF HOMELAND SECURITY PRIVACY IMPACT ASSESSMENT FOR COUNTER-UNMANNED AIRCRAFT SYSTEMS (C-UAS), DHS/ALL/PIA-085 *available at* https://www.dhs.gov/publication/dhsallpia-085-counter-unmanned-aircraft-systems-c-uas.
[8] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR THE OPERATIONS CENTER INCIDENT MANAGEMENT SYSTEM, DHS/TSA/PIA-029, *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.
[9] 49 U.S.C. § 114(f)
[10] *See* DHS/TSA-001 Transportation Security Enforcement Record System (TSERS), 83 FR 43888 (August 28, 2018) *available at* https://www.dhs.gov/system-records-notices-sorns.
[11] *See* DHS/TSA-002 Transportation Security Threat Assessment System, 79 FR 46862 (August 11, 2014), *available at* https://www.dhs.gov/system-records-notices-sorns.
[12] *See* DHS/TSA-011 Transportation Security Intelligence Services Operations Files, 75 FR 18867 (April 13, 2010), *available at* https://www.dhs.gov/system-records-notices-sorns.
[13] *See* DHS/TSA-019 Secure Flight Records, 80 FR 233 (January 5, 2015), *available at* https://www.dhs.gov/system-records-notices-sorns.
[14] *See* DHS/TSA-023 Transportation Security Administration Workplace Violence Prevention Program, 75 FR 8096 (February 23, 2010), *available at* https://www.dhs.gov/system-records-notices-sorns.

Characterization of the Information

Data elements associated with the new boards include:

- Secure Flight passenger data requests: subject/co-traveler name and any other identification information provided by the requesting agency, requester name/agency, name of TSA request reviewers (Privacy Office, Chief Counsel, Intelligence & Analysis).
- TSA Workplace Violence Prevention Program: full name of individuals involved in incidents of actual or alleged workplace violence as aggressor, victim, or witness, date of birth, gender, physical description, telephone number, email address, and types of injuries.
- Airline Operator Contacts: name, contact information, contact type/area of responsibility.
- National Capital Region Coordination Center Airspace Authorizations/Waivers: pilot/crew name contact information, aircraft registration or identifying data, as well as names and work contact information for public safety or law enforcement personnel associated with the operation.
- National Capital Region Coordination Center Uncrewed Aviation Systems: pilot and crewmember name/contact information, as applicable, as well as names/contact information for public safety or law enforcement personnel associated with the operation.

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

Mitigation: This risk is mitigated by only collecting information related to the Transportation Security Operations Center mission as the coordination center for transportation security incidents and operations. Some of the information is already collected by TSA and does not represent an expansion but rather centralizing existing information for coordination purposes or for improved management and administration of the information.

Uses of the Information

The information collected within WebEOC continues to be used for incident management, coordination, and situational awareness purposes. The Secure Flight passenger data requests board is designed to permit improved management and administration of external requests and TSA responses.

Notice

There are no changes regarding notice due to issuance of this Privacy Impact Assessment update.

Data Retention by the Project

WebEOC boards follow different National Archives and Records Administration (NARA) approved records schedules. The specific records schedule is determined by the type of data contained in the particular WebEOC board:

- Secure Flight passenger data requests are retained for five years (TSA 3700.3; General Records Schedule (GRS) 4.2 Item 050 NC1-64-77-1 Item 27).
- Workplace Violence Prevention Program records are retained for seven years (TSA 2800.13.1; N1-560-11-1 Item 1).
- Airline Operator contact information is destroyed when superseded (TSA 5000.15.2, General Records Schedule 6.5, Item 020; DAA-GRS-2017-0002-0002).
- NCRCC Airspace Authorization/Waivers records and Uncrewed Aircraft Systems records are retained for 10 years (TSA 3300.2.6-b; NA-560-05-1 Item 8; 3300.2.6b; N1-560-12-9 Item 1b).

Information Sharing

Information about passengers who are selected for enhanced screening under Silent Partner/Quiet Skies is not shared with parties external to DHS, unless: (1) the individual is believed to be in the Terrorist Screening Center's Terrorist Screening Database or on other watch lists; (2) the individual is believed to be involved in an incident for which external sharing is part of normal incident response protocols, such as when suspicious behavior rises to the level of a reportable event under the DHS Nationwide Suspicious Activity Reporting Initiative (DHS NSI) functional standard; or (3) the information is shared for redress, litigation, or oversight purposes. Disclosure is permitted under DHS/TSA-001 Transportation Security Enforcement Record System system of records notice, routine uses A, D, J, S, and U.

Secure Flight passenger data may be shared with external law enforcement or intelligence agencies where there is a nexus to transportation security or national security, exigent threat to life or similar extraordinary circumstances. Disclosure is permitted under the Privacy Act, 5 U.S.C. § 552a(b)(7) and DHS/TSA-019 Secure Flight Records system of records notice, routine uses 5 and 10.

Workplace violence prevention records may be shared under the Privacy Act and as described in the system of records notice: DHS/TSA-023 Transportation Security Administration Workplace Violence Prevention program.

National Capital Region Coordination Center Airspace Authorizations/Waivers information and National Capital Region Coordination Center Uncrewed Aviation Systems information will be shared with the Department of Transportation, and state and local agencies to

ensure safety and security in aircraft operations in the National Capital Region, and with other agencies regarding persons who pose or are suspected of posing a risk to transportation or national security, or as otherwise permitted under the Privacy Act and as described in the system of records notice: DHS/TSA-002 Transportation Security Threat Assessment System.

Redress

Individuals may continue to request access to their information by contacting the TSA Freedom of Information Act Office:

Freedom of Information Act Officer
Transportation Security Administration
TSA-20
6595 Springfield Center Drive
Springfield, VA 20598 – 6020
FOIA@tsa.dhs.gov

Access may be limited pursuant to exemptions asserted under 5 U.S.C. § 552a(k)(1) and (k)(2). Individuals who are neither United States citizens nor Lawful Permanent Residents do not have legal rights under the Privacy Act to access information. TSA may choose to grant such access in certain circumstances. In addition, consistent with the Judicial Redress Act, nonimmigrants that are deemed "covered persons" of a designated country or regional economic integration organization may seek access under the Privacy Act for certain information determined to be "covered records."

Auditing and Accountability

Personnel must attend all required privacy and IT security training and read and understand all applicable policies, standards, and procedures before receiving authorization to use WebEOC. TSA users are required to complete annual privacy, IT Security, and Sensitive Security Information training through TSA's Online Learning Center (OLC) system to access the TSA network.

Procedures to determine which users may access the WebEOC system are documented in the system security plan. Program office supervisors perform WebEOC account management tasks for their group, including establishing individual accounts and group membership, and modifying or disabling accounts. WebEOC users only have access to the web boards to which they are assigned. Program office supervisors are responsible for ensuring WebEOC user accounts are current and properly assigned. User accounts are audited on a quarterly basis. Any account found with inaccuracies, not current, or not included in the quarterly audit is blocked from accessing the WebEOC system. WebEOC "privileged accounts" that allow for greater access and use of the WebEOC system and data are provided only to a limited number of technical support personnel

who have been determined to have a legitimate need for the specific additional capabilities within the system.

The WebEOC System owner and the TSA Privacy Office review and determine approval of: Interconnection Security Agreements (ISAs), Memoranda of Understanding (MOUs), and new datasets. The WebEOC system owner collaborates with TSA IT Information Assurance Division to ensure proper system documentation and approvals are completed prior to establishing new interconnections and/or sharing of data.

Contact Official

John Bogers
System Owner
Transportation Security Operations Center
DHS/TSA
TSA-ocims@tsa.dhs.gov

Responsible Official

Peter Pietra
Privacy Officer
DHS/TSA

Approval Signature

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

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717