Privacy Impact Assessment

for the

Amtrak Rail Passenger Threat Assessment

DHS Reference No. DHS/TSA/PIA-050

December 1, 2021

Homeland Security

Abstract

The Transportation Security Administration (TSA) is responsible for security in all modes of transportation, including surface modes such as rail. Amtrak is a national passenger rail operator managing more than 300 trains a day to more than 500 destinations in the United States and Canada. To assess the operating environment from a risk perspective, Amtrak has requested that TSA assess the use of Amtrak trains by known or suspected terrorists. To conduct the assessment, Amtrak will provide TSA with rail passenger personally identifiable information (PII) collected over the course of several months for TSA to match against the Threat Screening Center's (TSC) Terrorist Screening Database (TSDB), commonly known as the "watchlist." TSA is conducting this Privacy Impact Assessment (PIA) pursuant to the E-Government Act of 2002 because this assessment entails a new receipt of personally identifiable information on members of the public for watchlist matching.

Overview

Following the September 11, 2001 terrorist attacks, Congress created the National Commission on Terrorist Attacks upon the United States (9/11 Commission).[1] The 9/11 Commission investigated the facts and circumstances relating to the attacks, and issued its report[2] in which it recognized that transportation involves more than just aviation, noting that "about 6,000 agencies provide transit services through buses, subways, ferries, and light-rail service to about 14 million Americans."[3] The 9/11 Commission also recognized that "opportunities to do harm are as great, or greater, in maritime or surface transportation" as they are in aviation.[4] As early as 2007, Congress suggested the possibility of a security watchlist system for Amtrak.[5] More recently, in the TSA Modernization Act, Congress said Amtrak should consider a passenger vetting system to enhance passenger rail security.[6]

The Aviation and Transportation Security Act requires TSA to "assess threats to transportation";[7] and "carry out such other duties, and exercise such other powers, relating to transportation security as the [Administrator] considers appropriate."[8] Amtrak serves over 30 million customers traveling to more than 500 destinations in 46 states, the District of Columbia

[1] Title VI, Intelligence Authorization Act for Fiscal Year 2003, Pub. L. 107-306 (116 Stat. 2383, Nov. 7, 2002).
[2] The 9/11 Commission Report is available at http://www.9-11commission.gov/.
[3] Report, p. 390-1.
[4] Report, p. 391.
[5] Title XV "Surface Transportation Security" of the Implementing Recommendations of the 9/11 Commission Act of 2007, codified at 6 U.S.C. § 1164.
[6] Federal Aviation Administration Reauthorization Act of 2018, P.L. 115-254, Division K, Title I (may be cited as the TSA Modernization Act). This assessment is being done independently of the TSA Modernization Act.
[7] 49 U.S.C. § 114(f)(2).
[8] 49 U.S.C. § 114(f)(15).

and three Canadian provinces, on more than 21,400 miles of routes.

Amtrak has requested that TSA assess the use of Amtrak trains by known or suspected terrorists for rail transportation. To the extent it is available, Amtrak will provide historical passenger manifests for several months on routes in the Northeast corridor to TSA. The manifests will contain first and last name and date of birth for passengers who have provided that data to Amtrak. In addition, where available, Amtrak may also provide additional data elements that passengers have provided on an optional basis or as part of frequent passenger Guest Rewards accounts. These additional data elements may include but not exceed: middle initial; billing address; phone; email; ticketed origin/destination; and actual origin/destination. TSA will match the passenger information against the Terrorist Screening Database to identify possible known or suspected terrorists.[9] TSA will not provide individual personally identifiable information on any known or suspected terrorist to Amtrak; instead, TSA will provide only statistical analysis regarding watchlist matching.

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?

The Aviation and Transportation Security Act requires TSA to "assess threats to transportation";[10] and "carry out such other duties, and exercise such other powers, relating to transportation security as the Administrator considers appropriate."[11] Title XV "Surface Transportation Security" of the Implementing Recommendations of the 9/11 Commission Act of 2007 provides for consultation between the Department of Transportation and TSA to upgrade Amtrak's security systems.

Amtrak has the authority to collect and share passenger information with the TSA pursuant to its broad and independent operating authority established by Congress under the Rail Passenger Service Act of 1970, Pub. L. 91-518, 84 Stat. 1328 (1970) (current version at 49 U.S.C. § 24101) (including the authority to "carry out strategies to achieve immediately maximum productivity and efficiency consistent with safe and efficient transportation" 49 U.S.C. § 24101(c)(3)). In addition, under Title 49 U.S.C. §§ 24305 and 28101, Congress authorized Amtrak to make and carry out appropriate agreements, to conduct research, development, and demonstration programs related to its mission, and to stand up its own police force to protect Amtrak employees, passengers,

[9] For more information about the Department's use of the Terrorist Screening Database, *see* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR THE DHS WATCHLIST SERVICE, DHS/ALL/PIA-027 (2016 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.
[10] 49 U.S.C. § 114(f)(2).
[11] 49 U.S.C. § 114(f)(15).

customers, and property. Under its police powers, the Amtrak Police Department can assess passenger information and request assistance from partner law enforcement agencies.

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

DHS/TSA-011 Transportation Security Intelligence Service (TSIS) Operations Files, 75 Fed. Reg. 18867 (April 13, 2010).[12]

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

Yes. TSA will use the Vetting and Credentialing System (formerly known as Transportation Vetting System) which has received an Authority to Operate (ATO) and is in an Ongoing Authorization status.

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

Yes. Information for this effort will be retained for two years in accordance with N1-560-04-10

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.

The collection is not covered by the Paperwork Reduction Act because TSA is not collecting or sponsoring the collection of any information.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Amtrak will provide historical passenger manifests for rail travel for several months for routes in the Northeast corridor. The personally identifiable information provided by Amtrak will consist of first and last name and date of birth for each passenger for which Amtrak has those data elements. In addition, Amtrak may have additional data elements that were provided by the passenger on an optional basis or as part of its frequent passenger Guest Rewards accounts that

[12] *See* DHS/TSA-011 Transportation Security Intelligence Service Operations Files, 75 Fed. Reg. 18867 (April 13, 2010), *available at* https://www.dhs.gov/system-records-notices-sorns.

will be provided to TSA to assist TSA in confirming watchlist matches. These additional data elements may include but not exceed: middle initial; billing address; phone number; email address; ticketed origin/destination; and actual origin/destination. TSA will conduct a match against the Terrorist Screening Database and retain possible match results for the assessment but will not provide the personally identifiable information of these results to Amtrak. In addition, during the process of resolving potential matches, TSA may share potential match information with the Threat Screening Center to obtain assistance in confirming whether the match is an actual match.

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

Amtrak collects certain passenger information from its reservations systems and other data it holds for frequent passengers. The primary sources of information for the assessment include Amtrak and the Threat Screening Center. If there is a possible, but inconclusive, match between Amtrak provided data and data held by the Threat Screening Center, TSA may collect open source information or commercial data to assist in verifying the validity of the possible watchlist match. For example, commercial data might be used to provide an address for a passenger that is a partial match to a watchlisted individual. Likewise, open source information, including publicly available social media, might provide information that confirms or eliminates a potential match with a watchlist record containing derogatory information.

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

In addition to the information provided by Amtrak, TSA may use information from commercial sources or publicly available data for this assessment if it would assist with resolving inconclusive watchlist matches.

2.4 Discuss how accuracy of the data is ensured.

Amtrak will deliver the passenger information, which is initially provided by passengers or other individuals making reservations for a passenger. TSA is unable to ensure the accuracy of any passenger information that is provided to Amtrak and then onwards to TSA. Initial automated watchlist match results will undergo analysis by TSA analysts to confirm a match. Personally identifiable information on matches will not be provided to Amtrak.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that limited information provided by Amtrak will result in inaccurate watchlist match results.

Mitigation: This risk is partially mitigated. TSA mitigates this risk to individual privacy through limitations placed on the use of the information. Because this assessment only involves historical travel, and only statistical information is provided to Amtrak, any potential incorrect match to a watchlist has no impact on the individual. TSA will coordinate with the Threat Screening Center to ensure the accuracy of the watchlist matching process and minimize the possibility of an inaccurate watchlist match.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

TSA will use the Amtrak passenger information to assess the possible use of Amtrak trains by known or suspected terrorists for domestic travel and TSA's capability to conduct watchlist matching for rail passengers.

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. TSA uses the information only to make subject based searches of Amtrak passengers who've made reservations to travel between a subset of stations against the watchlist.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. There are no other DHS components involved in this assessment.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information collected from Amtrak will be used for purposes other than the assessment.

Mitigation: This risk is partially mitigated. This Privacy Impact Assessment, the Memorandum of Understanding executed between TSA and Amtrak, and TSA policies regarding the protection and handling of Sensitive Personally Identifiable Information (SPII) ensure appropriate protection and use limitation of the data. Further, TSA does not currently maintain records on Amtrak passengers, so TSA only uses this information for this assessment. TSA will provide information on potential matches to the Threat Screening Center in order to obtain assistance in confirming a match, which may result in the Threat Screening Center using the information on a confirmed Known or Suspected Terrorist (KST) for purposes beyond this assessment. Data for passengers that are not a watch list match is retained for statistical purposes related to this project, but otherwise not used for any other purpose.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Prior to the start of the assessment, Amtrak will provide notice to its passengers through its privacy policies that are posted on its public website about sharing data with TSA. TSA will receive passenger data for historical travel only; however, TSA will provide notice about the receipt of historical data through the publication of this Privacy Impact Assessment.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

TSA does not provide opportunities for individuals to consent to uses, decline to provide information, or opt out of the assessment. Amtrak policies regarding its information collection are available at www.amtrak.com/planning-booking/policies/privacy-policy.html.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not know that their information may be shared with TSA.

Mitigation: This risk is partially mitigated. This Privacy Impact Assessment and publication of an updated Privacy Policy on Amtrak's website provide notice that Amtrak will be sharing passengers' information with TSA. The assessment will be based on several months-worth of historical data from the Northeast corridor; as only historical data is used neither TSA nor Amtrak are able to provide notice to passengers prior to the original collection. This Privacy Impact Assessment also provides notice that TSA will be sharing with Amtrak only statistical data that will not have personally identifiable information for any match results. In addition, Amtrak will update its Privacy Policy to reflect its sharing of passenger information with TSA. This Privacy Impact Assessment and the updated Privacy Policy will be completed before the collection of any data used for this assessment.

Section 5.0 Data Retention by the Project

5.1 Explain how long and for what reason the information is retained.

All records associated with this transportation security assessment project, including the records provided by Amtrak, will be retained for two years (N1-560-04-10, Item 7).

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the data used for the assessment may be retained longer than necessary.

Mitigation: This risk is mitigated. TSA will only maintain the information upon which the assessment is based in accordance with the approved records retention schedule of two years. TSA will ensure proper retention through manual processes outlined in standard operating procedures for this program.

Section 6.0 Information Sharing

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.

TSA may share potential and confirmed watchlist match information with the Threat Screening Center and with other law enforcement agencies pursuant to established routine uses. TSA also may share potential match information with the Threat Screening Center as part of the resolution process to confirm the match.

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

TSA will share information externally pursuant to established routine uses in the DHS/TSA-011 Transportation Security Intelligence Service (TSIS) Operations Files System of Records Notice (SORN).

Routine use G permits disclosing information to "To an appropriate federal, state, tribal, local, international, or foreign agency, including law enforcement, or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

Routine use I permits disclosing information to "To federal, state, local, tribal, territorial, foreign, or international agencies to provide intelligence, counterintelligence, information systems and transportation security information, and other information for the purpose of counterintelligence or antiterrorism activities authorized by U.S. law or Executive Order or for the purpose."

Routine use R permits disclosing information to "the appropriate federal, state, local, tribal,

territorial, foreign, or international agency regarding individuals who pose or are suspected of posing a risk to transportation or national security."

Routine use T permits the disclosing information to "a court, magistrate, or administrative tribunal where a federal agency is a party to the litigation or administrative proceeding in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings.

The foregoing routine uses assist TSA in performing its transportation security mission, including security assessments, and is compatible with the purpose for which the information is collected.

6.3 Does the project place limitations on re-dissemination?

No, but TSA will not provide personally identifiable information from the watchlist matching to Amtrak. Only aggregated information is shared to Amtrak.

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

This assessment will only disclose personally identifiable information to the Threat Screening Center as part of its automated watchlist matching, which logs the disclosure. Any disclosure made as a result of one of the DHS/TSA-011 Transportation Security Intelligence Service (TSIS) Operations Files System of Records Notice routine uses will be documented by the program office that provides the disclosure.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information will be inappropriately shared to external sources.

Mitigation: This risk is mitigated. TSA may share this information only in accordance with the Privacy Act. TSA will share information externally only in accordance with published routine uses under the DHS/TSA-011 Transportation Security Intelligence Service (TSIS) Operations Files System of Records Notice, including with the Threat Screening Center to confirm the accuracy of potential matches to the Terrorist Screening Database. For purposes of this assessment, TSA will only provide statistical information to Amtrak and will not provide personally identifiable information from any of the watchlist matches. Further, TSA has entered into a Memorandum of Understanding with the Threat Screening Center limiting TSA's use of the watchlist.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Individuals may request access to their data by contacting the TSA Freedom of Information Act Office, at Freedom of Information Act Officer, Transportation Security Administration, TSA-20, 6595 Springfield Center Drive, Springfield, VA 20598 - 6020 or via email at 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 their information. TSA may choose to grant such access in appropriate cases. 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 covered records.

Amtrak passengers may review Amtrak's access polices at https://www.amtrak.com/planning-booking/policies/privacy-policy.html.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals covered by the Privacy Act may submit a Privacy Act request as described in Section 7.1.

Amtrak passengers may review Amtrak's policy at https://www.amtrak.com/planning-booking/policies/privacy-policy.html.

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

This Privacy Impact Assessment provides notice on how to correct information held by TSA. The TSA website (www.TSA.gov) provides information on how to submit a Privacy Act request.

Amtrak passengers may review Amtrak's policies at http://www.amtrak.com/planning-booking/policies/privacy-policy.html.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will not have an opportunity to correct, access, or amend their records maintained by TSA.

Mitigation: This risk is mitigated. Individuals covered by the Privacy Act may seek access to TSA records by submitting a request under the Privacy Act, though some aspects of their record

may be exempt from access. This Privacy Impact Assessment provides notice of that process.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this Privacy Impact Assessment?

System administrators, security administrators, IT specialists, vetting operators, and analysts have access to the system in order to perform their duties in managing, upgrading, and using the system. Role-based access controls are employed to limit the access of information by different users and administrators based on the need to know the information for the performance of their official duties. TSA also employs processes to enforce separation of duties to prevent unauthorized disclosure or modification of information. No unauthorized users are permitted access to system resources. Strict adherence to access control policies is automatically enforced by the system in coordination with and through oversight by TSA security officers. Program management was involved in the conduct and approval of this Privacy Impact Assessment.

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

All users are required to complete annual TSA-mandated courses covering privacy. In addition, security training is provided, which helps to raise the level of awareness for protecting personally identifiable information being processed.

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 in writing and individual access is granted by an authorizing official. Access to any part of the system is approved specifically for, and limited only to, users who have an official need for the information in the performance of their duties. External storage and communication devices are not permitted to interact with the system.

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?

TSA will enter into a new Memorandum of Understanding for this assessment that describes the roles and responsibilities of TSA and Amtrak, particularly with respect to sharing of limited passenger data with TSA. The Memorandum of Understanding will also confirm that TSA will only provide Amtrak with statistical data, and Amtrak will not use the assessment results for operational law enforcement action against any specific individual. Any new information sharing,

uses, or access will be controlled in accordance with the foregoing Sections 8.2 and 8.3, and will be reviewed for compliance with this Privacy Impact Assessment.

Contact Official

Thomas Bush
Deputy Executive Assistant Administrator
TSA Operations Support
Thomas.Bush@tsa.dhs.gov

Responsible Official

Peter Pietra
Privacy Officer
TSA
TSAPrivacy@tsa.dhs.gov

Approval Signature

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

_____

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