Privacy Impact Assessment
for the

Insider Threat Unit Database

DHS/TSA/PIA-048

April 4, 2018

Contact Point
Serge Potapov
Office of Law Enforcement/Federal Air Marshals Service
Transportation Security Administration
InsiderThreatUnit@tsa.dhs.gov

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

Abstract

The Transportation Security Administration (TSA) protects the Nation's transportation systems to ensure freedom of movement for people and commerce. In support of this mission, the TSA Insider Threat Unit seeks to deter, detect, and mitigate insider threats from causing harm to the transportation domain. For purposes of the TSA Insider Threat Unit, "insiders" are, or present themselves to be, current or former transportation sector workers (including both TSA and private sector personnel) and individuals employed or otherwise engaged in providing services requiring authorized access to transportation facilities, assets, or infrastructure. Investigative files will be maintained in a database maintained by the Insider Threat Unit. This Privacy Impact Assessment (PIA) is conducted pursuant to the E-Government Act of 2002 because the database will include information on members of the public.

Overview

As discussed above, the TSA Insider Threat Unit seeks to deter, detect, and mitigate insider risks from causing harm to the transportation domain. For purposes of the TSA Insider Threat Unit, "insiders" are, or present themselves to be, current or former transportation sector workers (including both TSA and private sector personnel) and individuals employed or otherwise engaged in providing services requiring authorized access to transportation facilities, assets, or infrastructure. "Insider Threats" are "insiders" with the intent to cause harm to the transportation domain. The scope of the TSA Insider Threat program is accordingly broader than just a focus on TSA employees and contractors, or on TSA Information Technology infrastructure; it is instead designed to identify Insider Threat risk with the transportation modes that TSA regulates.

Information developed by the Insider Threat Unit will be used to deter, detect, and mitigate insider risks, and may be shared as appropriate with law enforcement and intelligence agencies, as well as affected transportation sector partners. A typical referral to the Insider Threat Unit may arise out of a security incident, hotline or informant tip, or other source, and will be assessed for insider risk nexus prior to acceptance for investigation. The Insider Threat Unit may investigate the potential threat, or refer the investigation to another component within TSA, or to external law enforcement if criminal activity is involved.

The Insider Threat Unit Database is the primary storehouse for reports and investigations for the Insider Threat Unit. It is used to track the status of a referral or incident involving a possible Insider Threat, as well as storing investigative material including personally identifiable information (PII) on the subject of the investigation and witnesses.

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?

TSA is responsible for security in all modes of transportation. This authority requires TSA to: (1) receive, assess, and distribute intelligence information related to transportation security,[1] (2) assess threats to transportation;[2] (3) develop policies, strategies, and plans for dealing with threats to transportation security;[3] (4) make other plans related to transportation security, including coordinating countermeasures with appropriate departments, agencies, and instrumentalities of the United States Government.[4] The Federal Aviation Administration (FAA) Extension, Safety, and Security Act of 2016 directs TSA to conduct or update an assessment to determine the level of risk posed by individuals with unescorted access to a secure area of an airport, directs TSA to review eligibility requirements for aviation worker credentials based upon current knowledge of insider threats and intelligence, and requires the development of model and best practices for aviation access control measures, and enhanced inspections of aviation workers.[5] Other authorities include 49 U.S.C.§ 44904, which requires joint assessments with the Federal Bureau of Investigation (FBI) regarding current and potential threats to the domestic air transportation system; and Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.[6]

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

DHS/TSA-001 Transportation Security Enforcement System (TSERS)[7] and DHS/ALL-038 Insider Threat System of Records.[8]

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

Yes. The system on which the Insider Threat Unit Database resides was granted a renewed Authority to Operate on October 31, 2017.

---

[1] 49 U.S.C. §114(f)(1).
[2] 49 U.S.C. §114(f)(2).
[3] 49 U.S.C. §114(f)(3).
[4] 49 U.S.C. §114(f)(4).
[5] FAA Extension, Safety, and Security Act of 2016, Pub. L. No. 114-190, § 3402(a)(1), 130 Stat. 615, 656 (2016).
[6] *See* https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net.
[7] DHS/TSA-001 Transportation Security Enforcement System (TSERS), 78 FR 73868 (Dec. 9, 2013).
[8] DHS/ALL-038 Insider Threat System of Records, 81 FR 9871 (Feb. 26, 2016).

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

Yes. National Archives and Records Administration General Records Schedule 5.6.

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.

This program does not require a collection of information under the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

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

The Insider Threat Database collects and maintains information on subjects and witnesses involved in Insider Threat reporting and investigation including TSA and private-sector personnel and members of the public, and may include such information as:

1. Name;

2. Driver's License number and Social Security number;

3. Passport number and citizenship;

4. Physical description and photograph;

5. Place and date of birth;

6. Gender;

7. Address;

8. Contact information;

9. Military status (branch, traveling on orders);

10. Watch list status;

11. Results of any law enforcement, criminal history record, public records, or open source checks;

12. Employment information and work history;

13. Security and access clearances and background investigations;

14. Travel records;

15. Information from other agencies (*e.g.*, FBI, Financial Crimes Enforcement Network (FinCEN)); and

16. TSA Information technology network activity information.

The database may also include other information relevant to the investigation including photographs or video, personnel records, or facility access records.

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

The Insider Threat Unit receives information from individuals who are subjects of investigations, from witnesses and informants, and from other governmental agencies and transportation sector partners. Information may be collected directly from the subjects involved, or indirectly from witnesses, informants, or other agencies and transportation sector partners. Information may also come from commercial or public sources as discussed below.

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

Yes. The Insider Threat Unit may use commercial sources such as Lexis-Nexis[9] for identification information or other purposes. It also uses publicly available data such as arrest records and criminal indictments to assist in investigating Insider Threats, as well as open source information such as public news and publicly-available social media content.[10]

2.4 Discuss how accuracy of the data is ensured.

The accuracy of information put into the database is important to support effective case investigation, tracking, and closure. Accuracy of information is maintained by allowing only a limited number of persons to enter data into the system and by assessing the facts of the potential insider threat before action is proposed.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of inaccurate information when it is collected from someone other than the individual, for example, from commercial or publicly available data.

[9] LexisNexis provides computer-assisted legal research for legal and public records-related information.
[10] There may be instances in which a member of the public reports private social media content to TSA (for example, a private chat in which a bomb threat is made), however, the Insider Threat Unit does not monitor non-public social media content.

Mitigation: This is a risk inherent in all law enforcement investigations and is mitigated by investigation before action is proposed. In some cases, information collected from other sources is entirely reliable; for example, if Closed-Circuit Television (CCTV) monitoring shows an individual leaving a security access point open and unsecured. Witness statements and third-party data are evaluated by investigators during the course of the investigation.

Privacy Risk: There is a risk that the information in the database could be used for purposes other than reporting, security matters, investigations, or law enforcement.

Mitigation: The privacy risk is diminished by limiting access to Insider Threat Unit members only. Also, only a limited number of unit members will conduct data entry. Additionally, all Insider Threat Unit Members are trained to safeguard sensitive information as part of their employment with TSA. Finally, password protection and username for log-in will be in place.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The Insider Threat Unit Database is the main records storage area for all Insider Threat referrals and investigations. The information is used to investigate Insider Threats, propose enforcement actions against the individual, assess threats to transportation, and develop strategies for addressing such threats across the transportation domain.

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. The Insider Threat Unit does not use technology to discover a predictive pattern or anomaly. It is developing a tool to prioritize investigations based on risk, but the tool does not seek to predict Insider Threat activity by any individual.

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

No. However, the TSA Insider Threat Unit works within the DHS Insider Threat Program on matters that fall within the scope of the DHS program in accordance with the DHS Insider Threat Operations Center Standard Operating Procedures. The DHS Insider Threat Program is limited to the detection, prevention, and mitigation of all threats that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the Department's mission, resources, personnel, facilities, information, equipment, networks, or systems. For DHS Insider Threat

Program purposes, an insider is defined as any person who has or who had authorized access to any DHS facilities, information, equipment, networks, or systems.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that PII may be disclosed without authorization.

Mitigation: The privacy risk is mitigated by limiting access to Insider Threat Unit members only. Unit members are assigned specific roles for data entry. Additionally, usernames and passwords are used. Finally, all members are trained on the appropriate safeguarding of PII and Sensitive Security Information (SSI) as part of their employment.

Privacy Risk: There is a risk that information gathered could result in an adverse action being taken against an individual outside the scope of the insider threat program. For example, analysis of information could result in identifying that an individual has committed a criminal act or misconduct, even if the same evidence does not indicate an insider threat.

Mitigation: This risk is mitigated by due process procedures in place when adverse action is taken, both within and outside of TSA. For example, TSA employees may file a grievance concerning disciplinary actions with the Office of Human Capital's National Resolution Center. Transportation Security Officers may appeal disciplinary actions to the Office of Professional Responsibility Appellate Board. Also, TSA's Security Threat Assessment Board, with representatives from TSA's Offices of Chief Counsel and Civil Rights & Liberties, reviews proposed adverse actions against transportation sector workers.

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.

Information collected from the individual is typically open and obvious and conducted by law enforcement such that notice is accomplished. However, the Insider Threat Unit does not provide notice to individuals prior to collection of information from other sources because the collection is part of a law enforcement or regulatory enforcement investigation. In some instances, there is no opportunity for notice, such as information developed from a security incident or provided by an informant. To the extent that the risk being investigated involves access to TSA IT assets, users are provided a notice at log-in that they are accessing a Government information system, have no reasonable expectation of privacy when using the system, that the Government may, without notice, monitor, intercept, search and seize any communication or data transiting or stored on the information system, and that the Government may disclose or use any communications or data transiting or stored on this information system for any lawful Government

purpose, including but not limited to law enforcement purposes. This PIA also provides notice of the collection of information.

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

Individuals (witnesses and subjects) interviewed as part of an insider threat investigation may decline to provide information but cannot limit the use of any information provided.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There may be a risk that the individual will not have notice of the collection.

Mitigation: Information collected directly from the individual is typically open and obvious, and the individual may decline to provide information. As a law enforcement or regulatory enforcement investigation, however, notice will likely not be provided on the development of the facts during the investigation. Information may be developed from a security incident or provided by an informant.

Section 5.0 Data Retention by the Project

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

Insider Threat Unit records are subject to the National Archives and Records Administration General Records Schedule 5.6: Security Records (July 2017), which mandates that (a) records pertaining to an "insider threat inquiry" are destroyed 25 years after the close of the inquiry; (b) records containing "insider threat information" are destroyed when 25 years old; (c) insider threat user activity monitoring (UAM) data is destroyed no sooner than 5 years after the inquiry has been opened, but longer retention is authorized if required for business use; and (d) insider threat administrative and operations records are destroyed when 7 years old.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that PII will be retained by TSA for longer than it is required, or needed.

Mitigation: This risk is mitigated by the fact that retention of PII within the Insider Threat Database is consistent with other systems holding the same or similar data. For example, the legal knowledge system used for prosecution of administrative and criminal matters retains records for ten years. By policy, the Insider Threat Unit performs an annual program assessment during which retention schedules can be implemented.

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.

The Insider Threat Unit may share information on insider threats with external law enforcement agencies, as well as appropriate transportation sector authorities and stakeholders. Sharing outside DHS will be done pursuant to the Privacy Act and routine uses published in the applicable system of records notice: DHS/TSA-001 Transportation Security Enforcement Record System (TSERS)[11] and DHS/ALL-038 Insider Threat System of Records.[12] Information is shared to investigate Insider Threats and address vulnerabilities.

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

The external sharing described in Section 6.1 is compatible with routine uses H, I, J, N, S, and X in DHS/TSA-001. These routine uses are designed to support sharing for the enforcement purposes for which the records were collected.

6.3 Does the project place limitations on re-dissemination?

Recipients of information are provided the information consistent with their authorities to investigate or take action on the referral. These recipients maintain the information consistent with their authorities. The Insider Threat Unit does not place a limitation on re-dissemination. Incident information may be SSI pursuant to 49 U.S.C. § 114(r), and re-dissemination is limited by the SSI regulation, 49 C.F.R. Part 1520.

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

Records of disclosure outside of DHS will be maintained manually within each investigative file.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy impact when PII is shared beyond DHS.

Mitigation: The risk associated with sharing information outside DHS is mitigated by sharing only as permitted by the Privacy Act of 1974 and for purposes compatible with the initial collection of the information. To the extent that Insider Threat Unit information is Sensitive

[11] DHS/TSA-001 Transportation Security Enforcement System (TSERS), 78 FR 73868 (Dec. 9, 2013).
[12] DHS/ALL-038 Insider Threat System of Records, 81 FR 9871 (Feb. 26, 2016).

Security Information under 49 USC 114(r), there are limitations on re-dissemination of the information. Recipients of information are provided the information consistent with their authorities to investigate or take action on the referral. These recipients maintain the information consistent with their authorities.

Section 7.0 Redress

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

While much of the information in the Insider Threat Unit Database is exempt from release under the Freedom of Information Act (FOIA) and Privacy Act, individuals may request access to their information under FOIA or the Privacy Act, if applicable, by contacting the:

TSA Headquarters FOIA Office
FOIA Officer
Transportation Security Administration
Arlington, VA 20598-6020

Access may be limited pursuant to exemptions asserted under 5 U.S.C. §§ 552a(j)(2), (k)(1), (k)(2), and (k)(5) for the systems of record under which the Insider Threat Unit operates. Access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation and reveal investigative interest on the part of TSA, as well as the recipient agency. Access to the records would permit the individual who is the subject of a record to impede the investigation and avoid detection or apprehension. Amendment of the records would interfere with ongoing investigations and law enforcement activities, and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated. The information contained in the system may also include properly classified information, the release of which would pose a threat to national defense and/or foreign policy.

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

Individuals may have an opportunity to correct their data if there is an investigative interview; otherwise, they may submit a Privacy Act request as described in Section 7.1.

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

TSA has published procedures to request amendment of records as described in Section 7.1.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: The risk that individuals cannot correct information about themselves.

Mitigation: Individuals may request access to and amend their personal information contained in Insider Threat Unit Database in accordance with the Privacy Act and the DHS Privacy Act regulation. However, much of the information in the system is exempt under FOIA and the Privacy Act as law enforcement or intelligence information, and may also be SSI exempt from disclosure under 49 U.S.C. § 114(r), which limits the ability of the individual to review information contained in the database. Harms are mitigated by investigative efforts that rely on accurate information before proposing adverse action against the individual. In addition, redress protections exist for the populations covered by this system.

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 PIA?

All Insider Threat Unit Database access is recorded and routinely analyzed and audited by personnel assigned to the Insider Threat Unit to ensure only authorized personnel are accessing and utilizing the system.

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

All TSA employees and contractors are required to take annual DHS privacy training.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

The Supervisory Air Marshal in Charge (SAC), or an authorizing official, decides when to create an account, and for whom access is granted. Users internal to DHS must have an official need for the information in the performance of their official duties.

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?

All requests for access are reviewed by the system owner, information system security officer, and the Security Assessments Section SAC. There are no information sharing agreements or MOUs, but such agreements would be reviewed by the system owner, information system security officer, program manager, component Privacy Officer, and counsel and then sent to DHS

for formal review.

Responsible Officials

Serge Potapov
Office of Law Enforcement/Federal Air Marshal Service
Security Services & Assessments Division
Transportation Security Administration

Approval Signature

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security