Privacy Impact Assessment
for the

TSA Office of Inspection Case Management

DHS/TSA/PIA-049

July 26, 2018

Contact Point
John Busch
Director
Office of Investigations, Transportation Security Administration
INV-Case Mgmt@tsa.dhs.gov

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

Abstract

The Transportation Security Administration (TSA) Office of Inspection (OOI) conducts covert testing of security screening operations; inspects TSA operations at airports, field offices, and other transportation entities; and investigates employee misconduct and program fraud, and violations of transportation security requirements. OOI's hotline referral and case management systems maintain Personally Identifiable Information (PII): (1) from individuals submitting information to OOI; and (2) on individuals designated as witnesses, victims, complainants, or subjects of an investigation. Since OOI Case Management maintains PII on members of the public, TSA is publishing a Privacy Impact Assessment (PIA) to assess the program's privacy impact on individuals, in accordance with Section 208 of the E-Government Act of 2002 and Section 222 of the Homeland Security Act of 2002.

Overview

The mission of the Transportation Security Administration (TSA) is to protect the nation's transportation systems to ensure freedom of movement for people and commerce. TSA's Office of Inspection (OOI) directly supports this mission by carrying out TSA's investigative and reporting requirements under 49 U.S.C. § 40113(a) and 49 U.S.C. § 46101, and in coordination with DHS's Office of the Inspector General (OIG) pursuant to the Inspector General Act of 1978, including investigations into employment misconduct.[1] OOI also assists in carrying out TSA's authority "to inspect, maintain, and test security facilities, equipment, and systems."[2] These efforts are intended to ensure the integrity of TSA operations and infrastructure. OOI investigations may lead to reports for DHS and TSA executive leadership, as well as Congress, the Government Accountability Office (GAO), and the Office of Management and Budget (OMB) to improve the effectiveness and efficiency of TSA's programs and operations.

OOI initiates investigations based on complaints that are directed to OOI; its own review of security incidents or regulatory violations; analysis of audit or covert operations data; and in response to requests from DHS's OIG, TSA management, or law enforcement and oversight officials. OOI investigations may be conducted into conduct by TSA employees or contractors, as well as other individuals whose activities fall within TSA jurisdiction such as transportation workers.

OOI receives tips and complaints directly from individuals or by DHS OIG referral. The DHS OIG may refer matters that either involve TSA employees or that fall within TSA's jurisdiction, such as a security violation at an airport. During the course of an investigation, OOI may collect PII, including Social Security numbers (SSN) and dates of birth (DOB), during interviews with members of the public that submit information to OOI or other individuals

[1] Pub. L. 95-452, 92 Stat. 1101 (1978).
[2] 49 U.S.C. § 114(f)(9).

designated as witnesses, victims, complainants, or subjects of investigations. This PII is stored within the OOI Case Management system, which is a module hosted on the TSA Office of Human Capital information technology system,[3] but otherwise has no interactions with the Human Capital system and is not accessible to unauthorized Human Capital system users.

The OOI Case Management module is a secure web portal accessible only to authorized OOI personnel in which case management and hotline referral cases are initiated. In addition, OOI uses the OOI Web Apps web portal, to manage administrative functions, including resource allocation, tracking investigation status, and processing office functions such as training reports, purchase requests, and on-boarding/out-processing of personnel. Only case numbers are manually imported from the case management module into OOI Web Apps. Agents then update OOI Web Apps with the type of case (criminal or administrative) and the number of hours worked.

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 (Pub. L. 107-71) gives TSA the authority to ensure the security all modes of transportation[4] including the authority "to inspect, maintain, and test security facilities, equipment, and systems."[5]

The Inspector General Act of 1978[6] grants DHS OIG the authority to conduct internal affairs investigations and, as amended by Section 812 of the Homeland Security Act of 2002 (Pub. L. No. 107-296), provides DHS OIG investigators with statutory law enforcement powers. Additionally, 49 U.S.C. § 114(p); 49 U.S.C. § 40113(a); 49 U.S.C. § 46101; and 49 U.S.C. § 44903(d) provide specific statutory authority for TSA to conduct investigations and designate employees as law enforcement officers.

[3] *See* DHS/TSA/PIA-023(a) Personnel Futures Program (October 13, 2017), *available at* www.dhs.gov/privacy.
[4] 49 U.S.C. § 114(d).
[5] 49 U.S.C. § 114(f)(9). See also 49 U.S.C. § 40113(a); 49 U.S.C. § 46101.
[6] 5 U.S.C. App. 3 § 2. The Inspector General Act of 1978 mandates Offices of Inspector General to: 1) conduct and supervise audits and investigations; 2) provide leadership and coordination and recommend policies for activities designed to promote economy, efficiency, and effectiveness, and to prevent and detect fraud and abuse; and 3) to provide a means for keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies and the necessity for and progress of corrective action.

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

DHS/ALL-020 Department of Homeland Security Internal Affairs and DHS/TSA-001 Transportation Security Enforcement Record System apply to the information TSA collects in order to conduct OOI inspections/investigations.[7]

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

Yes. The System Security Plan (SSP) documents the current and planned controls for the system and addresses security concerns that may affect the system's operating environment. The SSP includes user responsibilities, roles and limitations, and general security procedures for users and security personnel. Both the OOI Case Management module and OOI Web Apps have received an authority to operate.

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

Yes, OOI's retention schedule was approved by NARA in 2014. Information is retained up to 25 years depending on the type of record in accordance with NARA Authority N1-560-12-003.

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.

OOI does not engage in a "collection of information" that triggers the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

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

OOI may collect PII from members of the public that have reported allegations or individuals who have been designated as witnesses, victims, complainants, or subjects of investigations. The PII collected and maintained in OOI Case Management may include:

[7] *See* DHS/ALL-020 Department of Homeland Security Internal Affairs (April 28, 2014), 79 FR 23361, and DHS/TSA-001 Transportation Security Enforcement Record System (Dec 9, 2013), 78 FR 73868, *available at* www.dhs.gov/privacy.

- Full name;
- Social Security number (if provided);
- Date of birth;
- Photographs, video;
- Contact information (personal or business address, phone number, email);
- Gender;
- Race;
- Citizenship; and
- Case specific information such as background investigation results, fingerprints, security clearance status, medical records and workman's compensation information, training records, time and attendance, job duty performance records, firearms qualifications, and property management records.

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

OOI investigators collect information through a number of techniques, including hotline complaints and referrals from DHS OIG; as well as interviews of complainants, witnesses, victims, and subjects. Information may also be collected from third-parties with information relating to the subject of the investigation, such as medical providers in a workers compensation fraud investigation. Other sources of information include law enforcement personnel; reviews of records (*e.g.*, personnel files, contracts, time and attendance); reviews of public records and social media, including public and private content; and surveillance and consensual monitoring. OOI does not use keywords to monitor social media, rather, OOI agents may view publicly available information of an individual in an effort to validate a person's identity or to verify statements, such as having a relationship with one another.

When authorized by the head of OOI, and in accordance with DHS policy for operational use of social media,[8] private social media content may be viewed by OOI investigators during interaction with subjects or other investigative targets online through the use of aliases or "covers" in order to gather evidence during an ongoing investigation. Investigators may, through the use of undercover identities, join and particiate in chat rooms, blogs, or other types of of social media, when such participation is in furtherance of an official investigation and consistent with applicable federal law.[9] For example, an agent may during the course of a worker's compensation criminal

[8] DHS Instruction Number 110-01-001, "Privacy Policy for Operational use of Social Media" (6/8/2012).
[9] 49 U.S.C. § 114 (p)(2); 49 U.S.C. § 40113(a); 49 U.S.C. § 46101; and 49 U.S.C. § 44903(d).

fraud investigation, "friend" a suspect in order to view content that he or she is engaging in activities inconsistent with his or her physical restrictions. This activity is fully documented, including aliases and evidence gathered by the case agent and is included in the case file. When authorized, the OOI Computer Forensics Lab may analyze employees' computer hard drives or other digital media when information pertinent to an investigation is suspected of residing on the hardware.

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

Commercial or publicly available data may be used for investigative purposes, such as verifying addresses, identities, and contact information; tracing proceeds from illegal activities; and identifying possible witnesses.

2.4 Discuss how accuracy of the data is ensured.

OOI has an editing and review process for all investigation submissions. Agents are instructed to ensure accuracy and thoroughness through the investigative process; to consider confidentiality and security issues; to include disclosure caveats when appropriate; and to use electronic and other verification services to verify information as appropriate. The particular methods used to verify information compiled during the course of an investigation vary considerably depending on the type of investigation.

OOI verifies records by checking every incoming complaint to ensure that OOI or the DHS OIG has not received the same complaint previously. If so, OOI cross-references the two complaints; if not, the complaint is processed as a new entry. Information contained in the complaint is verified through the investigative process, which varies depending on the allegation and information at issue. OOI also updates the case management system with timely information on referrals, administrative actions, prosecutions, civil enforcements, and other information addressing the status of, or results of, an investigation or complaint review.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that inaccurate PII may be collected and maintained.

Mitigation: This risk is partially mitigated. Information collected by OOI via referrals or complaints is verified through the investigative process, which varies depending on the allegation or matter of complaint. Information received solely from social media is not used to initiate an investigation but may become part of an investigation, used to generate leads, or verify threats or risks. For example, in a workmans compensation fraud investigation, social media posts may reveal physical capabilities that are inconsistent with the compensation claim. OOI investigators

and inspectors receive extensive training on the sensitivity of investigative records and the need for accuracy therein.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

OOI uses the information maintained in the OOI Case Management System in order to conduct investigations and inspections related to TSA programs and operations. OOI's most common use of PII, including SSNs, is to verify the identities of subjects, complainants, witnesses, and third parties. OOI also uses SSNs to trace people, assets, and transactions depending on the specific allegation under investigation; as a search term when querying public and non-public databases for information relating to the case; and for other investigative purposes.

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. However, OOI may review data to track trends in terms of pending and completed investigations, types of complaints received, geographical locations, and other various factors in order to analyze office and personnel needs.

OOI also compiles information relating to investigative statistics for various reporting requirements, including but not limited to, the Semi-Annual Report to Congress required under the Inspector General Act.[10] OOI also reviews data to evaluate incoming complaints and to respond to various congressional, law enforcement and litigation requests, and information requests by other federal agencies and U.S. attorneys' offices during the course of a criminal prosecution or civil enforcement action.

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

No. Only TSA OOI personnel have access to OOI case management. OOI personnel may share final Reports of Investigations with TSA Employee Relations (ER), Office of Professional Responsibility (OPR), and Office of Chief Counsel personnel when necessary in the performance of their official duties. TSA ER is a department within the Office of Human Capital that is responsible for providing guidance and assistance in addressing employee misconduct, performance related issues, leave usage, grievances, and appeals.

[10] 5 U.S.C. App. § 5.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There are privacy risks associated with the potential for unauthorized disclosure or use inconsistent with the purpose of collection.

Mitigation: These risks are mitigated. OOI case management and all OOI investigative information are closely safeguarded in accordance with applicable laws, rules, and policies including Policy Directive 4300A, DHS Sensitive Systems. The OOI Web Apps System and HR portal are protected from unauthorized access through appropriate technical controls, including firewalls, access codes, and passwords. Each user has an account established within the HR portal and OOI Web Apps and gains access to the system using single-sign on authentication after having logged on to a secure network with a PIV Card and PIN. Each authorized user is provided with a limited roles-based permission level dependent upon his or her position and need-to-know. Furthermore, OOI investigators and inspectors receive extensive training on the appropriate collection, use, and disclosure of information related to investigations. All OOI employees are aware of the sensitivity of the OOI case data, investigative records, and information therein, as well as exemptions from disclosure through the Privacy Act of 1974 and the Inspector General Act of 1978 with respect to confidential informants, and other statutory and regulatory safeguards.

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.

The publication of this PIA, as well as the DHS/ALL-020 DHS Internal Affairs SORN, provide public notice of OOI's collection, use, and maintenance of PII. In most instances, individualized notice would interfere with OOI's ability to obtain, serve, and issue subpoenas, warrants, and other court documents that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence. In addition, providing notice to subjects of investigations would impede law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants. The Final Rule[11] for the DHS/ALL-020 DHS Internal Affairs SORN exempts this system from portions of the Privacy Act.

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

Individuals have the opportunity and right to decline to provide information depending on the nature of the investigation. OOI investigators undergo extensive training on interviewees'

[11] *See* Final Rule for Privacy Act Exemptions (August 24, 2009, 74 FR 42575).

rights and obligations in the context of responding to OOI investigative inquiries, and OOI has policies and procedures in place addressing interviewees' rights and obligations that vary depending on the type of investigation.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals are unaware of how investigative case files may be used and shared.

Mitigation: This risk is only partially mitigated. Authorized uses and routine sharing is provided in this PIA and in the applicable SORNs. Individuals who are questioned directly by TSA personnel have the ability to inquire as to use of the information they are providing.

Privacy Risk: There is a risk that individuals are not aware of how their private and/or restricted information on social media may be viewed and used by OOI Investigators.

Mitigation: This risk is only partially mitigated. TSA provides notice of authorized uses and routine sharing in this PIA and in the DHS/ALL-020 DHS Internal Affairs and DHS/TSA-001 Transportation Security Enforcement Records System SORNs; however, affirmative Privacy Act (e)(3) notice to individuals at the point of collection is not feasible on social media. Providing notice would interfere with OOI's ability to carry out its law enforcement function and compromise the existence of a confidential investigation. The final rule for the system of records officially exempts the system from notice portions if the Privacy Act.

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 as the information taken from open sources is typically posted by the individual and available to the general public. TSA assumes that individuals who post on open source venues are on notice that anyone, including government agencies such as TSA, may collect the information. PII is only gathered as evidence when it is relevant to the investigation. Information learned from open-sources, or from behind social media privacy settings if the individual has permitted access, is corroborated or evaluated for credibility prior to operational response. There may be incidental collection of PII of individuals who are not being investigated but who communicate on social media with persons who are bing investigated. Such incidental PII is retained in order to avoid tainting evidence but does not result in operational use.

Section 5.0 Data Retention by the project

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

OOI information, including PII, is retained up to 25 years depending on the type of record as approved by NARA.[12] Investigative case files, including PII, are maintained up to 25 years to

[12] *See* DHS/TSA Request for Records Disposition Authority Job Number N1-560-12-003 (November 1, 2014),

ensure records are available for any subsequent action, including but not limited to judicial appeals and related civil, criminal, or administrative actions. In addition, records may be needed in order to respond to inquiries from other law enforcement agencies related to law enforcement matters, and for background or clearance investigations.

- Investigative case files not referred to another internal or external agency for further investigation are cut-off at the end of the calendar year in which the case was closed, then destroyed five years after cut-off.
- Investigative case files referred to another agency are cut off at the end of the calendar year in which the case was closed and transferred to a Federal Records Center, then destroyed 25 years after cut-off.
- Hotline complaints are cut off at the end of the calendar year in which associated case is closed, then destroyed 10 years after cut-off.
- Analysis and review reports are cut off at the end of the calendar year in which the project is completed, then destroyed 20 years after cut-off.
- Fact finding and non-special reports are destroyed immediately when no longer needed for legal or operational purposes.
- Inspection case files are destroyed after completion of second succeeding office inspection or six years, whichever is longer.
- Trend analysis records are considered permanent.
- Programmatic and investigative correspondence files are not approved for disposition.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that OOI will retain more data than is necessary or will retain data for periods of time longer than approved.

Mitigation: This risk is mitigated. OOI mitigates excess data retention by limiting the data collection to the amount required to conduct its inspections and investigatons with a high level of confidence. OOI maintains information in accordance with the NARA-approved retention schedule and all employees are required to take records management training. OOI enforces its records schedule by reviewing investigative files annually and identifying the need for destruction of any investigative case file records that have been stored for five years since their cut-off date. OOI's data collection and retention practices relating to internal affairs are aligned with its purpose and mission, and are implemented accordingly.

available at https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0560/n1-560-12-003_sf115.pdf.

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.

Depending on the nature of the investigation, information may be shared with other federal or state internal affairs offices; state and local police departments; and other federal agencies, including the Federal Bureau of Investigation (FBI), Drug Enforcement Agency (DEA), United States Postal Inspection Service (USPIS), and Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF). If an investigation involves persons employed by other federal, state, or local agencies, information may be shared with those other agencies. If a case is referred for prosecution, information will be shared with the federal, state, or local prosecutors and/or law enforcement agencies. Information may also be shared with congressional committees with jurisdiction over matters under investigation.

OOI participates, on a regular basis, in interagency task forces involving federal, state, and local law enforcement agencies and may disclose information in accordance with the Privacy Act and the Inspector General Act, 5 U.S.C. App. 3, § 4(a)(4), which authorizes each IG to "coordinate relationships between such establishment and other federal agencies, state and local governmental agencies, and nongovernmental entities with respect to … the identification and prosecution of participants in such fraud or abuse."

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

The external sharing of information as described above is compatible with the purpose of collection. The purpose of DHS/ALL-020 Department of Homeland Security Internal Affairs SORN is to collect and maintain records concerning the internal affairs matters, specifically internal integrity or displinary inquiries, as well as internal reviews, inspections, or investigations conducted by TSA and the other DHS components. This SORN is intended to support and protect the integrity of departmental operations; to ensure compliance with applicable laws, regulations, and policies; and to ensure the integrity of DHS employees' conduct and those acting on behalf of DHS.

For example, under Routine Use A and for the purpose of ensuring compliance with applicable laws and regulations, OOI information may be shared with the "Department of Justice (DOJ) (including Office of the United States Attorneys) or other federal agency conducting litigation, or in proceedings before any court, adjudicative, or administrative body when it is necessary to the litigation and one of the following has a party to the litigation or has an interest in the case: (1) DHS or any component thereof; (2) any employee of DHS in his/her official capacity;

(3) any employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or, (4) the U.S. Government or any agency thereof."[13]

Routine Use G authorizes the sharing of information "to an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when 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."[14] This sharing is compatible with the purpose of collection: to ensure compliance with applicable laws, regulations and policies.

Finally, Routine Use H authorizes sharing with federal, state, local, tribal, territorial, foreign, or international agencies if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or the issuance, grant, renewal, suspension, or revocation of a security clearance, license, contract, grant, or other benefit; or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit. This sharing is compatible with the purpose of collection of ensuring the integrity of DHS employees' conduct and those acting on behalf of DHS.

Sharing with congressional committees with jurisdiction over matters under OOI investigation may be conducted as set forth in the Privacy Act, 5 USC §552a(b)(9).

6.3 Does the project place limitations on re-dissemination?

OOI does not place limitations on re-dissemination; however, information is shared primarily with other law enforcement and Government agencies whose personnel are familiar with the Privacy Act and other restrictions on release of information. To the extent information is designated Sensitive Security Information (SSI) under 49 USC §114(r), re-dissemination is limited by regulations found at 49 CFR part 1520. OOI notifies recipients of the confidential nature and disclosure restrictions through verbal statements, written markings on documents, and agency policies recognizing the confidential nature of such materials.

[13] *See* DHS/ALL-020 Department of Homeland Security Internal Affairs (April 28, 2014), 79 FR 23361, *available at* www.dhs.gov/privacy.
[14] *Id.*

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

OOI maintains an electronic log of any disclosures. The log contains the date, due date of the request, what information, case numbers if applicable, and name and address of the individual or agency to whom the disclosure is made. In most cases this disclosure is made upon a Freedom of Information Act (FOIA) request, for which a separate FOIA log is maintained.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that PII may be shared with persons without a need to know or recipients may not secure PII properly.

Mitigation: OOI properly marks all documents as to their sensitivity level and provides requirements for secure access along with the exchange. OOI uses appropriate transmittal mechanisms that vary depending on the nature of the information and vehicle by which it is transmitted. Also OOI's participation in interagency task forces involving federal, state, and local law enforcement agencies often are created pursuant to Memoranda of Understanding (MOU) and other formal or informal agreements. These MOUs cover the scope of information that may be shared, depending on the nature of the investigation, allegations under review, status of the agencies involved, and status of the investigation.

Section 7.0 Redress

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

Individuals may seek access to their information by submitting a request under the Privacy Act to the the TSA Headquarters Freedom of Information Act (FOIA) Office, at FOIA Officer, Transportation Security Administration, TSA-20, Arlington, VA 20598-6020. A request may also be submitted by fax at 571-227-1406 or by email at FOIA.TSA@dhs.gov. Instructions on how to request records from TSA may also be found here: https://www.tsa.gov/foia/requests. Access may be limited, however, since DHS has exempted the system of records[15] from certain Privacy Act access or amendment requirements.

Requests for information will be evaluated by DHS on a case-by-case basis to ensure that exemptions are only taken where the request meets the specific standards set forth in the Privacy Act of 1974.[16]

[15] *See* Final Rule for Privacy Act Exemptions (August 24, 2009, 74 FR 42575).
[16] 5 U.S.C. § 552a(j)(2) and (k)(2).

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

Individuals may seek to correct records by submitting a request pursuant to the Privacy Act. Instructions may be found at www.TSA.gov under the FOIA link in Section 7.1.[17] Note, however, that pursuant to the Privacy Act, DHS has exempted the system of records from certain access and amendment requirements. In the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

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

TSA provides information on submitting requests under the Privacy Act and Freedom of Information Act on its public website at www.TSA.gov.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will not be able to correct erroneous information.

Mitigation: This risk is partially mitigated. The routine uses, permissible sharing of PII, and access procedures are published in this PIA and the DHS/ALL-020 Internal Affairs and DHS/TSA-001 Transportation Security Enforcement Records System SORN in an effort to be as transparent as possible; however, as explained in the sections above, OOI investigation records are exempt from the notice, access, and amendment requirements of the Privacy Act. Requests for information will be evaluated by DHS on a case-by-case basis to ensure that exemptions are only taken where the request meets the specific standards set forth in the Privacy Act of 1974.

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?

As part of the internal technical controls within the OOI Case Management system, case files are restricted to those persons with a need to know. Each record has an audit log to track the modification and who made the changes (by person and date/time stamp). In addition, OOI employees and in particular, OOI investigators are trained in appropriate access to investigative information and paper investigative files that provides protection against misuse.

[17] https://www.tsa.gov/foia/requests.

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

All authorized users are notified during their on-boarding orientation of the confidential nature of the data and prohibitions against misuse and improper disclosure of OOI investigative data and paper investigative files. DHS OIG conducts an annual Security Awareness Session that addresses privacy issues, nondisclosure, methods of protecting data and outputs, and confidentiality and security concerns generally. All OOI Special Agents also receive specific direction through DHS OIG directives and manuals that address the unique privacy interests in investigative materials.

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

OOI has established procedures for granting access to investigative case files via the case management module that resides on the Office of Human Capital (OHC) information technology system. The OOI Investigations Division and certain authorized users from the Office of Human Capital may request access to the case management module with approval from the Investigations Division Director. Employees must first have an active Web Apps or OHC account, which serves as verification of the employee's assigned position, office or division, location, and whether or not the employee needs to access investigative case data. Then, once access to the case management module is granted, the user is assigned privileges specific to the employee's role in order to restrict access to pertinent case files, including the ability to read and write each case record. Access to investigative paper files is restricted to OOI investigations personnel assigned to the case, OOI management, and other OOI personnel, select Office of Professional Responsibility (OPR) and Office of Chief Counsel (OCC) personnel with a specific need-to-know in line with 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 MOUs, Task Force, and information sharing agreements are reviewed by OOI leadership and sent to DHS OIG for formal review. OOI may seek review by the Office of Chief Counsel, and consults the TSA Privacy Officer when privacy concerns arise.

Responsible Officials

John Busch, Director
TSA Office of Investigations
Department of Homeland Security

Approval Signature

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security