Privacy Impact Assessment
for the

DHS Traveler Redress Inquiry Program

DHS/ALL/PIA-002(b)

April 23, 2018

Contact Point
Deborah O. Moore
Branch Manager, Transportation Security Redress Branch
Transportation Security Administration
TRIP@DHS.gov

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

Abstract

In 2005, the Transportation Security Administration (TSA) created the Office of Transportation Security Redress (OTSR) to manage TSA's Traveler Identity Verification Program (TIVP). TIVP offered redress avenues for individuals who experienced aviation-related screening issues. In 2006, Secretary of State Rice and Homeland Security Secretary Chertoff launched a Joint Initiative[1] to provide a single point of contact for individuals seeking resolution of difficulties they may experience during travel screenings at transportation hubs and named TSA the program's executive agent. TSA designated OTSR, renamed the Transportation Security Redress Branch (TSRB), the managing office for the Department of Homeland Security's consolidated redress program, called the Traveler Redress Inquiry Program or "DHS TRIP."

DHS TRIP provides redress avenues to individuals who encounter travel-related screening difficulties. Applications for redress are managed in a secure, web-based database called the Redress Management System (RMS). DHS TRIP uses this system to manage inquiries from individuals who believe they have been unfairly or incorrectly delayed, denied boarding, or identified for additional security screening at U.S. airports, official ports of entry, and other transportation hubs. DHS TRIP works with relevant components and other federal agencies when necessary, such as the U.S. Department of State's (DoS) visa issuance and passport offices and the Federal Bureau of Investigation's (FBI) Terrorist Screening Center (TSC),[2] to properly respond to travelers' requests for redress. DHS TRIP is a privacy-sensitive system because it collects Personally Identifiable Information (PII) from members of the public; therefore, DHS must conduct a Privacy Impact Assessment (PIA) on the program in accordance with Section 208 of the E-Government Act of 2002. This PIA consolidates and supersedes previous DHS TRIP PIAs and TSA's TIVP PIA.[3]

Overview

DHS TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs or crossing U.S. borders. This includes watch list issues;[4] screening problems at ports of entry; and situations in which travelers believe they have been unfairly or incorrectly delayed, denied boarding, or identified for additional screening at our nation's airports, official ports of entry, or other transportation hubs.

---

[1] *See* "Rice-Chertoff Joint Vision: Secure Borders and Open Doors in the Information Age," Joint DoS/DHS announcement, January 17, 2006, at https://2001-2009.state.gov/r/pa/prs/ps/2006/59242.htm.
[2] *See* https://www.fbi.gov/about/leadership-and-structure/national-security-branch/tsc.
[3] *See* https://www.dhs.gov/publication/retired-pias for the original DHS TRIP PIA's and for TSA's TIVP PIA.
[4] The "watch list" includes the "No Fly," "Selectee," and "Expanded Selectee" components of the TSC's Terrorist Screening Database as well as other watch lists maintained by the Federal Government.

DHS components and offices that operate within DHS TRIP are TSA, U.S. Customs and Border Protection (CBP), U.S. Citizenship and Immigration Services (USCIS), U.S. Immigration and Customs Enforcement (ICE), and the Office of Biometric Identity Management (OBIM), as well as the DHS Office for Civil Rights and Civil Liberties (CRCL), and the DHS Privacy Office (PRIV). These DHS entities work with DoS visa issuance and passport offices and the FBI's TSC. These offices, collectively known as the DHS TRIP components, work collaboratively to address travelers' screening-related travel difficulties.

DHS TRIP facilitates efficient handling of redress requests, communication of redress results, and related information across DHS components, including DHS's redress oversight office, the the Office of Policy's Screening Coordination Office (PLCY/SCO). DHS TRIP collects individuals' information to determine which DHS component or other agency is best able to address the request and to resolve, when possible and appropriate, the underlying issue regarding the inquiry. DHS TRIP shares individuals' information with DHS TRIP components within the data system, as appropriate, in order to facilitate the appropriate review and response.

Individuals who wish to file for redress can complete an online application at https://trip.dhs.gov, or mail or email[5] a completed copy of DHS Form 591, *Travel Inquiry Form* (TIF).[6] On DHS Form 591, individuals must sign and date an acknowledgment that the information provided on the TIF is true, accurate, and provided voluntarily under penalty of perjury; this form may be submitted via email or mail. Each individual filing a request receives a system-generated Redress Control Number (RCN) to track the request's status. The applicant must submit all required documentation within 30 days of filing the TIF. If supporting documents are not received within 30 days, DHS TRIP will suspend work on the request until the documents are received. Once all required documentation is received, DHS TRIP reviews the request and forwards it to the appropriate DHS TRIP component for review. The component reviews the case, researches the matter, and, when appropriate, makes changes to the component's systems that may be causing a travel issue. When the component notifies DHS TRIP that its review is complete, DHS TRIP conducts a final quality-assurance review of the case, closes it, and sends the applicant a letter indicating the resolution.

There are three categories of PII that DHS TRIP collects from individuals: (1) the individual's contact information to enable DHS TRIP to communicate with the individual; (2) specific information about the individual's experience to help DHS TRIP identify which component is best able to address the request; and (3) personal information and documentation to authenticate the individual. The collection of this PII involves significant privacy risks to the individual; therefore, DHS TRIP instituted privacy risk mitigation strategies following the Fair

[5] Mail: DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901 Arlington, VA 20598-6901; or email: TRIP@dhs.gov.
[6] *See* https://trip.dhs.gov/DHS_Form_591-Traveler_Inquiry_Form.pdf.

Information Practice Principles (FIPPs) to secure individuals' information and protect their privacy.[7]

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?

Title IV of the Intelligence Reform and Terrorism Prevention Act of 2004[8] directs that airline passengers who are delayed or prohibited from boarding an aircraft as a result of a screening program determination have a means to appeal the determination and correct erroneous information. Furthermore, TSA[9] and DHS[10] are responsible for "establishing a timely and fair process for individuals identified as a threat ... to appeal the determination and correct any erroneous information."

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

DHS/ALL-005 DHS Redress and Response Records System[11] applies to the information DHS collects in order to process TRIP requests.

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

Yes. Information contained in the DHS TRIP system is safeguarded in accordance with the Federal Information Security Management Act of 2002 (FISMA).[12] The system has undergone a full Security Authorization Process and has operated under an ongoing authorization since 2006.

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

In accordance with General Records Schedule (GRS) 5.1, Item 20, all government information and individual subject data are destroyed or deleted once entered or otherwise incorporated into the master DHS TRIP database, called the Redress Management System (RMS). Paper-based records are destroyed 90 days after receipt. Information in RMS is maintained for 99 years after issuance of the final agency decision for a redress request, or for seven (7) years after

---

[7] *See* Privacy Policy Guidance Memorandum 2008-01, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*.
[8] *See* Pub. L. 108-458, Section 4012(a)(I).
[9] *See* 49 U.S.C. § 44903(j)(2)(G).
[10] *See* 49 U.S.C. § 44909(c)(6)(B).
[11] *See* DHS/ALL-005 DHS Redress and Response Records System, 72 FR 2294 (Jan. 18, 2007).
[12] *See* Pub. L. 107-347.

TSA learns that the individual is deceased, upon which TSA is authorized to delete the record, in accordance with NARA Authority N1-560-07-02/B/1.

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 OMB Control number assigned to this collection is 1652-0044, which expires March 31, 2019.

Section 2.0 Characterization of the Information

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

DHS TRIP collects information directly from the individual, or from the individual's attorney or other representative with the individual's authorization. There are three categories of information collected, used, and disseminated: (1) contact information; (2) information about the individual's travel difficulty; and (3) information/documentation to verify the individual's identity. DHS TRIP also maintains information about the response to the redress request from the responding agency.

A. Contact Information for the Applicant and Applicant Attorney or Representative, if applicable.

- Applicant Full Name
- Applicant Mailing Address
- Applicant Physical Address
- Applicant Telephone number and Email Address
- Attorney/Representative Name
- Attorney/Representative Firm Name
- Attorney/Representative Address
- Attorney/Representative Telephone Number
- Attorney/Representative Email Address

B. Information about the individual's experience to assist DHS TRIP identify which component is best able to address the request;

- For incidents related to flight:
  - Flight Date
  - Airport
  - Airline
  - Flight Number
  - Domestic or International Flight
  - Which if any of the following scenarios describe the applicant's experience (applicants must check one):
    - Subjected to additional pre-boarding screening
    - Denied Boarding
    - Delayed by an official/agent
    - Received "Secondary Security Screening Selection (SSSS)" on boarding pass
    - Unable to print boarding pass and directed to ticket counter
    - Other
- For incidents related to Ports of Entry, Immigration, Customs or Border Patrol:
  - Date of Entry
  - Name of Airline or Ship
  - Port of Entry
  - Flight or Cruise Number
  - Departure Date (from U.S.)
  - United States Airport
  - United States Port of Departure
  - Name at Entry into U.S., and
  - Which if any of the following scenarios describe the applicant's travel experience (applicants must check one):
    - Referred to secondary screening

- Denied Entry
- Denied Electronic System for Travel Authorization (ESTA)
- Foreign student or exchange visitor unable to travel due to status
- Given an information sheet by a CBP Officer
- Other

C. Identity Information and Documentation to verify the applicant's identity. All forms of identification must be unexpired, government-issued, and photograph-bearing:

- Information
  - Applicant Full Name, and Other Names used
  - Date of Birth
  - Place of Birth
  - Gender
  - Height
  - Weight
  - Hair Color
  - Eye Color
  - U.S. Person (U.S. Citizen or Lawful Permanent Resident) or Non-U.S. Person
- A copy of at least one of the following types of documentation:
  - Passport
  - Passport Card
  - Driver's License
  - Certified Birth Certificate (for minors only)
  - Military Identification Card
  - Government ID Card
  - Certificate of Citizenship
  - Naturalization Certificate

- Immigrant/Non-Immigrant Visa
- Alien Registration/Permanent Resident Card number
- Secure Electronic Network for Travelers Rapid Inspection (SENTRI)
- NEXUS
- Free and Secure Trade (FAST)
- Global Entry
- Border Crossing Card

D. DHS TRIP also maintains information about the responsible agency's response to the redress request including the results of any matching against a U.S. Government watch list.

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

The source of the information is the individual submitting a request for assistance or the individual's representative. Individuals submit their information through a secure, online application or by completing a hard-copy of the TIF and submitting it by mail or email.

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

DHS TRIP does not use information from commercial sources or publicly available data in the processing of redress requests.

2.4 Discuss how accuracy of the data is ensured.

DHS TRIP collects PII directly from the individual seeking redress, or his or her representative, greatly reducing the likelihood of erroneous PII. The individual must also provide proof of his or her identity by submitting at least one identity document (see Section 2.1.C). The documentation is necessary to ensure that the person requesting redress is who he or she says he or she is and is not providing fraudulent or incorrect information. Such documentation helps correctly identify the individual and facilitate the redress process, particularly in instances of misidentification. Verification of the identity and supporting documentation will also help substantiate when there is a need to correct information held by DHS TRIP components. DHS TRIP personnel conduct two levels of quality review to ensure that the data appearing on the

submitted identity documentation has been entered accurately into the Redress Management System.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: DHS TRIP may collect more information than necessary to respond to a redress request.

Mitigation: DHS TRIP attempts to only collect PII that is directly relevant and necessary to fulfill a redress request. The DHS TRIP website provides a Frequently Asked Questions (FAQ) section that is designed to address questions that do not require an individualized response to help reduce the number of requests and the need to collect PII.

Privacy Risk: DHS TRIP makes a redress determination based on incorrect data.

Mitigation: Collecting information directly from the individual greatly reduces the likelihood of erroneous PII. The individual must also provide proof of his or her identity by submitting a copy of at least one identity document. The documentation is necessary to ensure that the person requesting redress is who he or she says he or she is and is not providing fraudulent or incorrect information. Such documentation will help correctly identify the individual and facilitate the redress process, particularly in instances where the delay or issue may be attributed to a misidentification. Verification of the identity and supporting documentation will also help identify when there is a need to correct information held by DHS or one of the participating agencies.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

DHS TRIP uses the PII to coordinate the DHS redress process and to simplify the process for travelers wishing to submit a redress request. Information collected is used to identify the most appropriate DHS TRIP component to address the redress request. DHS TRIP maintains in RMS all traveler requests and the component responsible for handling the request. DHS TRIP also tracks case progress and final resolution to provide metrics for responding to requests; to identify areas in need of additional support, which may lead to corresponding resources requests; and to develop best practices regarding the DHS redress process. Once intake information is complete, DHS TRIP transfers this information to the appropriate component, which will follow its own process to address the inquiry using the information provided by the individual.

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.

DHS TRIP does not use information in order to discover or locate a predictive pattern or anomaly. The information provided is only used to help respond to a request for redress; to provide aggregate metrics about the program's performance; and to help DHS identify improvements needed within its screening and redress procedures.

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

In the ordinary course of administering DHS TRIP, it is expected that the information will be shared with relevant components and programs within DHS where it is necessary to process and address a redress request. Components operating within this system are: TSA; CBP; USCIS; ICE; PLCY/SCO; OBIM; CRCL; and PRIV. Programs within these components that participate in DHS TRIP include TSA's aviation and passenger screening programs and CBP's processing of international travelers. The information DHS TRIP receives from individuals may be shared with DHS employees and contractors who have a need for the information in the performance of their official duties as they relate to processing and responding to a request for redress.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: DHS TRIP information may be accessed without authorization.

Mitigation: Records in the system are maintained in a secure, password-protected electronic system that utilizes security hardware and software to include multiple firewalls, active intruder-detection, and role-based access controls. Additional safeguards vary by component and program. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include restricting access to authorized personnel who have a need-to-know, using locks and password-protection identification features.

Privacy Risk: Information may be used for matters unrelated to the redress request.

Mitigation: Information technology security controls are in place within the system to protect the confidentiality, availability, and integrity of the personal data in DHS TRIP, including role-based access controls that enforce a strict need-to-know policy. In addition, administrative controls, such as periodic monitoring of logs and accounts, help to prevent and/or discover unauthorized access or improper use of information. Audit trails are maintained and monitored to track user access and unauthorized access attempts. In addition, users are trained on proper information handling procedures and that the information is to be used for redress purposes or

related authorized purposes, such as litigation, responding to Congressional inquiry, and national security investigations.

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.

Individuals are provided notice of the collection before and when they choose to submit an inquiry or request for redress to DHS TRIP. This PIA provides notice of the collection, its purpose, and all authorized uses of the information while DHS/ALL-005 Redress and Response System of Records[13] articulates all individuals and categories of records covered by the system as well as all routine uses of information therein. There is also notice provided at the time of collection by a Privacy Act Statement included in the online application and hard-copy form. Furthermore, individuals must acknowledge that they are voluntarily submitting PII themselves and that the information provided is accurate.

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

The redress process is voluntary so individuals have the right to decline to engage in the process or limit the information they provide for review. Providing less information than requested may make resolution of the matter more difficult or impossible as noted in the application's Privacy Act Statement.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Individuals may not be aware of all the ways their PII may be used and shared.

Mitigation: This PIA provides notice of the collection, its purpose, and all authorized uses of the information while DHS/ALL-005 Redress and Response System of Records articulates all individuals and categories of records covered by the system as well as all routine uses of information therein. There is also notice provided at the time of collection by a Privacy Act Statement on the website and the hard-copy TIF. Furthermore, individuals must acknowledge that they are voluntarily submitting PII for redress purposes and that the information provided is accurate.

[13] *See* DHS/ALL-005 DHS Redress and Response Records System, 72 FR 2294 (Jan. 18, 2007).

Section 5.0 Data Retention by the Project

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

In accordance with General Records Schedule (GRS) 5.1, Item 20, all government information and individual subject data are destroyed or deleted once entered or otherwise incorporated into the master DHS TRIP database. Paper-based records are destroyed 90 days after receipt. All information in RMS is maintained for 99 years after issuance of the final agency decision for a redress request, or seven years after TSA learns that the individual is deceased, after which TSA is authorized to delete the redress record in accordance with NARA authority N1-560-07-002/B/1. The 99-year retention period for DHS TRIP electronic records is necessary in case the individual experiences any additional travel difficulties throughout his or her lifetime.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Informaiton may be retained for longer than necessary.

Mitigation: DHS TRIP attempts to only collect PII that is directly relevant and necessary to fulfill a redress request and ensures that all PII collected is accurate. Collecting information directly from the individual greatly reduces the likelihood of erroneous PII. The DHS TRIP website provides an FAQ section that is designed to address questions that do not require an individualized response to help reduce the number of requests and the need to collect PII. If the FAQ section does not eliminate the need to submit a redress request, individuals will be asked to review a series of traveler experience screening statements to help DHS TRIP identify and assess the nature of the redress issue. The redress application and the information it collects are then tailored to the individuals' responses and the type of travel issue; thus, minimizing the data needed to address an individual's specific request. Finally, TSA follows the NARA-approved GRS for all information that is submitted to DHS TRIP.

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 information collected and retained by DHS TRIP may need to be shared with other federal agencies when necessary to address an individual's redress request. DHS TRIP may share information provided by an individual seeking redress with other federal departments and programs such as the DoS's passport or visa offices or the DOJ's TSC, in order to determine the appropriate response. For example, DHS TRIP may exchange information with the DoS when the redress request pertains to visa issuance or a passport program. Likewise, information may be shared with DOJ when the information may be used to distinguish the identity of the individual

seeking redress from that of another individual included on a U.S. Government watch list, or to determine whether the traveler's experience was based on incorrect information.

Additionally, limited information may be shared with non-governmental entities when necessary for the sole purpose of effectuating an individual's redress request. For example, if an individual has been cleared and distinguished from an individual who is known or suspected to be a threat to aviation security, TSA will share that individual's name and appropriate associated information with the airlines to prevent future delays and disruptions for that individual while traveling. Other types of routine information sharing are outlined in the DHS/ALL-005 Redress and Response System of Records.[14]

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

In the DHS/ALL-005 DHS Redress and Response System of Records, Routine Uses A, B, C, D, E, F, and I allow DHS to share DHS TRIP records or information with external organizations as described above. These disclosures are compatible with the original collection because Title IV of the Intelligence Reform and Terrorism Prevention Act requires that travelers who experience difficulties with any DHS security screening procedure have a mechanism to inquiry about or apply for redress, and to correct any erroneous information which may have resulted in delay or misidentification. For example, Routine Use A allows DHS TRIP to disclose records to other "federal, state, territorial, tribal, local, international or foreign government agency or entity for the purpose of consulting with that agency: (1) to assist in making a determination regarding the redress for an individual in connection with the operations of a DHS component or program; (2) for the purpose of verifying the identity of an individual seeking redress in connection with the operations of a DHS component or program; or (3) for the purpose of verifying the accuracy of information submitted by an individual who has requested such redress on behalf of another individual." Routine Use C allows DHS TRIP to share information with "third parties lawfully authorized in connection with a Federal Government program, which is authorized by law, regulation, or rule, but only the information necessary and relevant to effectuate or to carry out a particular redress result for an individual and disclosure is appropriate to enable these third parties to carry out their responsibilities related to the Federal Government program…."[15]

6.3 Does the project place limitations on re-dissemination?

DHS TRIP has entered into a Memorandum of Understanding with relevant Federal agencies, including the TSC, FBI, Department of Justice, and Department of State, created in consultation with privacy and civil liberties officials of each agency as well as the Privacy and Civil Liberties Oversight Board, that require the parties to appropriately handle and secure PII.

[14] *See* DHS/ALL-005 DHS Redress and Response Records System, 72 FR 2294 (Jan. 18, 2007).
[15] *See* DHS/ALL-005 DHS Redress and Response Records System, 72 FR 2294 (Jan. 18, 2007).

All federal agencies are subject to the Privacy Act of 1974 and must handle TRIP information accordingly. DHS TRIP does not place other limits on re-dissemination.

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

The DHS TRIP Director maintains a record of all requests for DHS TRIP information and any/all resulting external disclosures. RMS maintains an accounting of all information shared with DoS and DOJ, the DHS TRIP components that are not part of DHS.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information may be lost or disclosed inappropriately during external sharing.

Mitigation: Any external sharing of information is done through a secure data network, and all disclosures are documented.

Privacy Risk: There is a risk that data shared by TRIP with external partners will be used beyond the original purpose of collection.

Mitigation: TRIP shares data with external agencies that have a need to know and for purposes compatible with the original collection pursuant to an MOU. TRIP users do not receive access unless they perform an authorized function within the system, and are trained on appropriate use of the information. This mitigates the risk of unauthorized disclosure by requiring a trained employee with access to the information to review the information before sharing the information with an external agency.

Section 7.0 Redress

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

All individuals may request access to information submitted as part of their redress requests by submitting a Freedom of Information Act (FOIA) to the TSA FOIA Branch. U.S. Citizens and Lawful Permanent Residents may also submit a Privacy Act request to the TSA FOIA Branch. Requests may be submitted online at https://www.tsa.gov/foia/requests, by email to FOIA@tsa.dhs.gov, or regular mail to the following address.

Transportation Security Administration
TSA-20, East Tower
FOIA Branch
601 South 12th Street
Arlington, VA 20598-6020

In addition, individuals covered by the Judicial Redress Act[16] may seek access to their records.

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

After submitting a redress request through the DHS TRIP website, an individual, regardless of citizenship or immigrations status, may request to modify or correct information he or she originally submitted by sending the correct information in an email to DHS TRIP. The program will then send notification of receipt to the individual. DHS TRIP will review the revised information and determine if any additional component or agency should also review or update information pertaining to the individual's redress issue. Individuals eligible under the Privacy Act and the Judicial Redress Act may also submit a request to correct their records.

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

Individuals are notified of how to correct their information on the DHS TRIP website. Records access and amendment procedures also are listed in the DHS/ALL-005 DHS Redress and Response System of Records.[17]

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: An individual may be unaware of his or her right of access, amendment, and an accounting of DHS TRIP disclosures.

Mitigation: DHS TRIP does not offer redress for any travel redress decisions beyond rights of access, amendment, and accounting of disclosures afforded by the Privacy Act and FOIA. An individual who is dissatisfied with the results of his or redress request may have the opportunity to submit supplementary information based upon redress procedures, if any, of the component or agency responsible for responding to the request. If the applicant experiences new travel-related screening difficulties, he or she may submit a new application. In general, DHS TRIP provides a redress process that furthers the privacy interest of the individual by providing an easy-to-use website that facilitates the submission and processing of redress requests. Since DHS TRIP collects PII directly from the individual, the risk of collecting inaccurate or irrelevant information should be minimized.

[16] *See* https://www.justice.gov/opcl/judicial-redress-act-2015.
[17] *See* DHS/ALL-005 DHS Redress and Response Records System, 72 FR 2294 (Jan. 18, 2007).

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?

RMS is secured against unauthorized access and use through a layered, defense-in-depth security approach involving procedural and information security safeguards. Only DHS personnel and personnel of participating agencies with responsibilities related to processing and responding to redress requests will be able to access the data stored on the system.

Employees or contractors are assigned roles for accessing the system based on their function. The system administrator grants access on a "need-to-know" basis. The system administrator also manages the activation or deactivation of accounts and privileges as required, helping to ensure the system's compliance with privacy and security policies. DHS TRIP ensures personnel accessing RMS have security training commensurate with their duties and responsibilities. Personnel also have any necessary background investigations and/or security clearances for access to the system.

Contractors who are hired to perform many of the administrative or information-technology maintenance and security monitoring tasks have access to the DHS TRIP system in order to perform their official duties. All contractors performing such work are subject to the Homeland Security Acquisition Regulation (HSAR) and Federal Acquisition Regulation[18] (FAR), requiring contractors be favorably investigated and adjudicated for suitability and complete privacy training before they may be permitted to work in DHS TRIP and access RMS.

RMS uses an audit trail feature to track any changes to the data and to track access to the system. The system has the capability to track individual record access and modifications by user name as well as the time/date stamp associated with that action. The system administrator will regularly review the audit system logs.

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

DHS government and contractor personnel associated with DHS TRIP are required to complete initial and refresher privacy training on an annual basis. Compliance with this requirement is audited and personnel access can be denied if individuals are non-compliant. In addition, security training is provided regularly, which helps raise the level of awareness for protecting PII.

[18] *See* 48 C.F.R. § 30.

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

In order to perform their duties in managing, upgrading, and using RMS, system administrators, security administrators, IT specialists, redress analysts, intelligence analysts, call center employees, and any other DHS TRIP and component redress office employees, detailees, or contractors and personnel from participating federal agencies with a need to know the information to perform their official duties associated with this program may have access to the system. Automated role-based access controls are employed to limit the access of information by different users based on the need to know. Role-based controls are based on the policy of "Least Privilege," which enforces the most restrictive set of rights and privileges or access needed by users based on their roles. 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 the system administrator.

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 new access to the system or DHS TRIP information are reviewed by the DHS TRIP Director. Information sharing agreements or MOUs are reviewed by the TRIP Director, Office of Chief Counsel, DHS SCO, and the TRIP Board which has representatives from each DHS Component.

Responsible Officials

Deborah O. Moore
TSRB Manager/DHS TRIP Director
Transportation Security Administration
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