Privacy Impact Assessment

for the

Technical Reconciliation Analysis Classification System (TRACS)

DHS Reference No. DHS/OBIM/PIA-003(a)

July 17, 2020

Homeland Security

Abstract

The U.S. Department of Homeland Security's (DHS) Office of Biometric Identity Management (OBIM) operates the Technical Reconciliation Analysis Classification System (TRACS), an information management tool used for reporting and analysis of the Automated Biometric Identification System (IDENT) records to support OBIM's information sharing coordination activities with external agencies and foreign partners. These partners are charged with national security, immigration, or law enforcement responsibilities. OBIM is retiring and reissuing the previously published Privacy Impact Assessment (PIA) to identify new functionality supported by TRACS.

Overview

OBIM operates TRACS, an information management tool primarily used for analysis of records associated with IDENT[1] and its successor system, currently in development, called the Homeland Advanced Recognition Technology (HART).[2] OBIM maintains the Department's primary repository of biometric information held by DHS in connection with varied missions and functions, including law enforcement; national security; immigration screening; border enforcement; intelligence; national defense; and background investigations relating to national security positions, and credentialing consistent with applicable DHS authorities.

OBIM is retiring and reissuing the previously published TRACS PIA,[3] as functions previously carried out by the original TRACS PIA, specifically overstay analysis and support for credentialing of employees, are no longer supported by TRACS. Also, since last publication, TRACS now fully supports international data sharing efforts, redress functions, and reporting and analysis functions.

The specific personal identifiable information (PII) in a TRACS record varies depending upon what information the source records contain. PII contained in TRACS may include: name, date of birth (DOB), country of birth, document numbers/types, encounter date, reason fingerprinted, foreign partner unique identifier, fingerprint identification number (FIN), immigration information, border crossing information, and free-form text fields for analyst

[1] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[2] HART, IDENT's replacement IT system, is a centralized DHS-wide biometric database that contains limited biographic and encounter history information needed to place the biometric information in proper context. HART will store and process biometric data (digital fingerprints, iris scans, facial images (including a photo)) and link these biometrics with biographic information pursuant to the data owner's authorities and policies for use, retention, and sharing of information. Deoxyribonucleic acid (DNA) retention is not included in HART Increment 1. *See* DHS/OBIM/PIA-004 Homeland Advanced Recognition Technology System (HART) Increment 1, *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[3] TRACS PIA was originally published June 6, 2008, *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

findings. TRACS does not contain any biometric data and is not the original source for any PII. OBIM analysts either import data from IDENT and foreign partner correspondence or manually enter all PII into the system. Appendix A further describes other DHS and non-DHS information sources.

Internal and external agencies do not directly use or have access to TRACS. The users of the TRACS database only include a limited number of OBIM employees and contractors. OBIM analysts upload data from IDENT to TRACS to search, create reports, and query information from IDENT. IDENT supports OBIM's information sharing coordination activities with external agencies and foreign partners.

Types of TRACS Generated Records

Records in TRACS are generated in three different ways: 1) OBIM manually imports bulk biographic data of IDENT system records that have matched to an inbound foreign partner query onto Excel spreadsheets; 2) OBIM receives foreign partner bulk data extracts of that country's corresponding identifiers, labeled as fields in Excel spreadsheets, and manually enters that information into TRACS; and 3) OBIM manually enters redress requests from the DHS Traveler Redress Inquiry Program (DHS TRIP)[4] system and additional any other redress requests to review data inaccuracies.

1) Foreign Partner Query: OBIM analysts import records from IDENT into TRACS whenever a foreign partner query of IDENT results in a match. These spreadsheets are automatically imported into TRACS without manipulating the data. The import feature allows the OBIM analysts who use TRACS to confirm the file before completing the import. Once imported, OBIM analysts perform applicable system searches (described below and as referenced in Appendix A) and record their findings in TRACS. In turn, OBIM analysts provide the requestor a summary of the findings per match (as permissible under DHS policy, statutes, and information sharing agreements (ISAA)) via encrypted email and manually record in TRACS when it was sent, match or no-match, the requestor who received the email, and the OBIM analyst who sent it. As previously referenced, the only automated process is the import of spreadsheets and email generation.

2) Foreign Partner Extracts: Once OBIM notifies a foreign partner of an IDENT match, the partner may request more information about the subject of the match. The foreign partner may submit a spreadsheet with the corresponding matching identifiers to OBIM; analysts then manually upload the data into TRACS. This process triggers OBIM analysts to search applicable authorized systems listed in the appendix and record the findings in TRACS. OBIM analysts then provide the requestor the findings via encrypted email as permissible

[4] *See* DHS/ALL/PIA-002 DHS Traveler Redress Inquiry Program (TRIP), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

under DHS policies, statutes, and agreements, and manually record when the email was sent, the name and organization of the requestor to whom it was addressed, and the name of the OBIM analyst who sent it.

3) DHS TRIP Redress Requests: Lastly, OBIM analysts manually enter redress requests from DHS TRIP[5] and non-DHS TRIP redress requests into TRACS. Redress requests include corrections to IDENT records. Redress request information added to TRACS includes date the request was sent, the requesting individual's PII, the submitting agency of the request, the names of the OBIM personnel who reviewed the request, and findings for possible resolution of the requests. OBIM personnel submit case findings to TRIP for those requests made via TRIP. OBIM's Biometric Support Center (BSC) makes all applicable corrections and closes the case. For redress request records received outside of TRIP, OBIM responds to the individual/agency who submitted the request via mail, email, or fax.

TRACS Searches

Once OBIM imports records into TRACS, OBIM analysts log into the system and conduct an additional review to determine the individual's immigration status, criminal history, travel history, among other items, for reporting back to the partner. OBIM must conduct manual search and analysis since IDENT is not able to send automated responses for certain types of information that are covered under DHS's ISAAs. OBIM analysts search immigration and law enforcement databases and manually input relevant data into TRACS. OBIM may search a variety of databases including: U.S. Customs and Border Protection's (CBP) Arrival and Departure Information System (ADIS),[6] CBP's TECS (not an acronym),[7] U.S. Citizenship and Immigration Services's (USCIS) Central Index System (CIS),[8] USCIS's Person Centric Query Service (PCQS),[9] ICE's EID Arrest Guide for Law Enforcement (EAGLE),[10] ICE's ENFORCE Alien Removal Module (EARM),[11] Department of State's (DOS) Consular Consolidated Database (CCD),[12] Department

[5] *See* DHS/ALL/PIA-002 DHS Traveler Redress Inquiry Program (TRIP), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.
[6] *See* DHS/CBP/PIA-024 Arrival and Departure Information System (ADIS), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[7] *See* DHS/CBP/PIA-021 TECS System: Platform, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[8] *See* DHS/USCIS/PIA-009 Central Index System (CIS), *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[9] *See* DHS/USCIS/PIA-010 Person Centric Query Service, *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[10] *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID), *available at* https://www.dhs.gov/privacy-documents-ice.
[11] *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID), *available at* https://www.dhs.gov/privacy-documents-ice.
[12] Consular Consolidated Database (CCD) PIA, *available at* https://foia.state.gov/_docs/pia/consularconsolidateddatabase_ccd.pdf.

of Justice's (DOJ) Executive Office for Immigration Review (EOIR) (accessible through USCIS PCQS),[13] and Interpol's e-ASF2 system.[14]

Information Sharing Coordination

When a partner sends an automated query to IDENT, and IDENT makes a biometric match, OBIM manually imports the relevant IDENT biographic information (e.g., name, DOB, FIN, and encounter information) into TRACS. OBIM analysts review the query and forward it to the Component data owner to add any additional biographic information they may choose to disclose.

When the foreign partner submits a follow-up request for more information, OBIM analysts conduct a review to search immigration and law enforcement systems, as authorized, and draft case findings which are manually uploaded to TRACS. The case findings include details behind adverse actions, travel history, and hits to IDENT fast matchers.[15] OBIM manually shares the case findings, as authorized, with the foreign partner. OBIM records the dates and times of all query-related transactions and uploads the final DHS response to an encrypted email, which is sent to the partner. The foreign partner uses these findings to determine if the individual they encountered is eligible for a certain immigration benefit or for admissibility, or a law enforcement action, as appropriate.

Redress

OBIM uses TRACS to record and process redress requests from internal DHS or other U.S. Government (USG) agency users. OBIM analysts use TRACS to review IDENT records on individuals who have submitted redress requests and to correct possible mismatches. For example, if an individual's fingerprint record has been incorrectly linked to another person's record, the individual may be sent to secondary inspection, which can cause inconvenience and hardship. If the individual submits a redress request, OBIM uses TRACS to record a summary of the findings and document the resolution of the case. Redress resolution facilitates the travel process for the

[13] EOIR PIA, *available at* https://www.justice.gov/sites/default/files/opcl/docs/eoir_pia.pdf.
[14] Interpol's e-ASF2 system, *available at* http://www.interpol.int/INTERPOL-expertise/Data-exchange/I-24-7. OBIM uses system data in the Stolen and Lost Travel Documents and Nominal Data databases within Interpol to obtain information on stolen documents and international criminals that have been watch listed. *See* information on how INTERPOL processes data in I-24/7, *available at* http://www.interpol.int/content/download/13042/90082/version/30/file/20%20e%20rpd%20update%20(14y2089)%20(or).pdf.
[15] Records on IDENT's biometric fast matchers, previously referred to as the "IDENT Watchlist," is a sub-set of IDENT records maintained for rapid matching and access of information on persons of interest including wants and warrants from federal, state, local, tribal, and international law enforcement agencies through the FBI; known or suspected terrorists (KSTs); deported felons and absconders; sex offender registrants; gang-related records; subjects who have violated U.S. immigration laws; subjects who have been denied a biometric visa by DOS; and other persons of interest to DHS.

individual the next time he or she enters the country, and ensures that OBIM records are as accurate, complete, and up-to-date as possible.

OBIM analysts manually enter in TRACS redress requests cases from the Transportation Security Administration (TSA) Records Management System (RMS) of DHS TRIP[16] assigned to OBIM employees and non- DHS TRIP redress requests. OBIM analysts enter the date the request was sent, the requesting individual's PII, the agency submitter of the request, the names of the OBIM personnel who handled the request, and search findings for possible resolution of the requests. OBIM updates information contained in IDENT consistent with the resolution. If there is a discrepancy in another system, OBIM notifies the system owner. Once a resolution is determined, OBIM submits case findings to DHS TRIP RMS and makes applicable corrections for biometric mismatches. The cases are then considered resolved and closed.

Reporting Functions and Administrative Tasks

OBIM uses TRACS to support administrative tasks and multiple reporting functions like the Director's Operations Status Report (DOSR), Executive Performance Report (EPR), and Information Bulletins. None of these reports contain PII, but rather discuss statistics such as number of transactions per week and average redress response times.

Internal and external agencies do not directly use or have access to TRACS. A limited number of OBIM analysts use the TRACS database. The information contained in TRACS may be shared with DHS Components and other federal agencies, such as DOS, and foreign partners, in accordance with applicable ISAAs, DHS policies, and statutes.

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 data is collected and maintained in TRACS under the authority provided by:

- 6 U.S.C. secs. 202 and 482;
- 8 U.S.C. secs., 1365a, 1365b, 1379, 1722, 1731, and 1732;
- 13764 (82 FR 8115), Homeland Security Presidential Directive 12 (HSPD-12): Policy for a Common Identification Standard for Federal Employees and Contractors (Aug. 27, 2004);
- HSPD-11: Comprehensive Terrorist-Related Screening Procedures (Aug. 27, 2004); and

[16] *See* DHS/ALL/PIA-002(b) DHS Traveler Redress Inquiry Program, *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

- National Security Presidential Directive/NSPD-59/HSPD-24: Biometrics for Identification and Screening to Enhance National Security (June 5, 2008).

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

The Enterprise Biometric Administrative Records (EBAR) SORN[17] covers administrative records maintained in TRACS. It covers the Fingerprint Identification Number, Encounter Identification Number, and other transactional information owned by OBIM. DHS Components, such as CBP, ICE, Federal Emergency Management Agency (FEMA), TSA, USCIS, and U.S. Coast Guard (USCG), are the original collectors and owners of the biometrics. Component biometrics are governed by their own source system SORNs. Records from external federal partners include information from non-DHS systems of records. The source system SORNs referenced are outlined in Appendix A. Records that DHS receives from external entities, like international partners are covered by the DHS/ALL-041 External Biometric Records System of Records.[18]

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

Yes. OBIM has completed a System Security Plan (SSP) for the TRACS system on September 2019. OBIM is currently working on receiving a new Authority to Operate (ATO).

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

OBIM is currently developing the transactional record systems retention schedule. Once complete, OBIM will submit to NARA for approval.

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.

TRACS does not collect information directly from the public and therefore is not covered by the PRA.

[17] DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR) System of Records, 85 FR 14955 (Mar. 16, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.
[18] DHS/ALL-041 External Biometric Records (EBR) System of Records, 83 FR 17829 (Apr. 24, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.

Section 2.0 Characterization of the Information

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

TRACS contains data extracted from IDENT and received from foreign partners. TRACS contains information on non-U.S. citizens (e.g., visitors or applicants for entry to the U.S. or to a foreign partner country, such as individuals who have submitted a visa application to the United Kingdom (U.K.) through the U.K. Home Office Visa Services Project,[19] or those who a foreign partner believes are subjects of interest for law enforcement or immigration processing). TRACS may also contain data on individuals who are lawful permanent residents and those who have become U.S. citizens as they have moved through the immigration process, as well as some data on native born U.S. citizens.[20]

For individuals identified above, TRACS contains the following biographic information and associated biometric indicator data:

- **Biographic data** includes name, aliases, DOB, country of birth, gender, nationality, document country, document number, document type, encounter date/date fingerprinted, reason fingerprinted, location fingerprinted, passport number, candidate organization/unit/subunit (OUS), alien registration number, derogatory information (DI),[21] DI description,[22] DI shared,[23] IDENT fast matchers status information, DHS TRIP/redress number;[24] and free-form text fields that allow OBIM to record employee notes based on searches and comment information;
- **Foreign partner data** may include country, foreign partner unique identifier, foreign partner transaction number, and search code; and
- **Biometric indicator data:** TRACS does not contain any actual biometric data, only biometric indicators, including FIN or the encounter identification number (EID).

To support the data sharing initiatives, OBIM gathers and compiles immigration, law enforcement, and national security information about a particular individual that can be disseminated, as

[19] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) Appendices, *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.
[20] *Id*.
[21] A set of data related to negative or criminal information associated with an encounter. Derogatory Information is information which potentially justifies unfavorable suitability, fitness, or security adjudication and such information may prompt a request for additional investigation or clarification for resolution of an issue. DI may include information submitted from the Department of Defense (DoD), the Federal Bureau of Investigations (FBI), the Department of State, INTERPOL, international country partners, and DHS Components, specifically ICE and CBP.
[22] Description of the derogatory information for that encounter.
[23] Indicates what data can and cannot be shared depending on the project and existing filters.
[24] TRIP number references the redress case number in the TRIP system.

missions dictate and per data sharing rules already existing in IDENT, to users internal and external to DHS across the immigration, law enforcement, and border enforcement communities. OBIM's findings are maintained in TRACS. OBIM is not creating new information. Instead, OBIM compiles information from a variety of immigration, national security, and law enforcement databases and shares the resulting case summaries with authorized users. These case findings are used to make accurate determinations in the course of a law enforcement, immigration, or border enforcement action.

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

The data contained in TRACS derives primarily from IDENT and its replacement system HART. TRACS also contains data provided from a foreign partner subsequent to a biometric match in IDENT. TRACS does not collect any data directly from individuals; but rather, it relies on the collection of data from various external and DHS internal organizations. TRACS contains information on individuals who are potentially subjects of interest for further analysis by DHS and foreign partner agencies.

DHS Sources

IDENT: IDENT stores and processes biometric data—digital fingerprints, photographs, iris scans, and facial images, and limited associated biographic information. Digital fingerprints and associated biographic information assist in OBIM's ability to establish identities. IDENT serves as a biographic and biometric repository for DHS. DHS Components; DOS (information for visas and background investigations); DOJ; Department of Defense (DOD); other federal, state, local, tribal, and foreign governments; foreign law enforcement agencies; and noncriminal justice origins collect information that is stored in IDENT.[25]

IT Systems Used for OBIM Searches

When IDENT makes a match to a foreign partner query, OBIM analysts manually import the matched biographic data into TRACS. In addition to the limited biographic data elements that may be shared from IDENT, the foreign partner may request more information from the USG agency that owns the data. OBIM manually receives the request and then disseminates it to the appropriate USG agency for their consideration and response. Case summaries of shareable information pertaining to IDENT matches are stored in TRACS. The information is derived from system searches for immigration and criminal history from the following databases.[26]

[25] Non-criminal justice data providers are defined as those who use criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances. 42 U.S.C. sec. 14616.
[26] *See* Appendix A for additional information.

- OBIM IDENT;[27]
- CBP ADIS;[28]
- CBP TECS;[29]
- USCIS CIS;[30]
- USCIS PCQS;[31]
- ICE EAGLE;[32]
- ICE EARM;[33]
- DOJ EOIR (via PCQS);[34]
- DOS CCD;[35] and
- Interpol's e-ASF2 system.[36]

External Foreign Sources

Foreign law enforcement and immigration officials collect information and share it with the U.S. Government in accordance with ISAAs, U.S. laws, and additional implementation documentation. TRACS ingests limited foreign partner data elements in order to support the following international data sharing efforts, as noted in Appendix A.

United Kingdom Home Office's Visa Services Project

The U.K. enacted legislation requiring the submission of biometric data from almost all individuals filing visa applications for entry into the U.K. Officials from the U.K. and DHS have agreed that individuals who are physically located in the United States and in Jamaica may provide

---

[27] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.
[28] See DHS/CBP/PIA-024 Arrival and Departure Information System (ADIS), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[29] *See* DHS/CBP/PIA-021 TECS System: Platform, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[30] See DHS/USCIS/PIA-009 Central Index System (CIS), *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[31] *See* DHS/USCIS/PIA-010 Person Centric Query Service, *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[32] *See* DHS/ICE/PIA-015(j) EID Arrest Guide for Law Enforcement (EAGLE), *available at* https://www.dhs.gov/privacy-documents-ice.
[33] *See* DHS/ICE/PIA-015(d) Enforcement Integrated Database (EID) ENFORCE Alien at Removal Module Update, *available at* https://www.dhs.gov/privacy-documents-ice.
[34] Executive Office for Immigration Review (EOIR) PIA at www.justice.gov/sites/default/files/opcl/docs/eoir_pia.pdf.
[35] Consular Consolidated Database (CCD) PIA at https://foia.state.gov/_docs/pia/consularconsolidateddatabase_ccd.pdf.
[36] International Criminal Police Organization (Interpol) e-ASF2 system at www.interpol.int/INTERPOL-expertise/Data-exchange/I-24-7.

the requisite biometrics and limited biographical information at USCIS Application Support Centers (ASC) for forward transfer to the U.K. in support of the adjudication of applications for visas. USCIS, working in conjunction with OBIM, uses subsystems of IDENT and other systems for the U.K. Home Office Visa Services Project.[37] For the U.K. Visa Services Project, OBIM will receive biographic information based on biometric matches from U.K. visa applicants. OBIM then queries those matches against the IDENT list of subjects of interest. OBIM will provide the results from the query back to the U.K. for purposes of visa adjudication. OBIM analysts will use TRACS to record the request and responses for this project. For up-to-date information on the U.K. Home Office's Visa Service Project please refer to the IDENT PIA Appendices.[38]

Migration 5

The Migration 5 (M5) is a forum for cooperation on migration and border security between the countries of Australia, Canada, New Zealand, the United Kingdom, and the United States (collectively called the M5 partners). M5 partners, including the United States, exchange biometric information in specific immigration cases where: (1) the identity of the individual is unknown or uncertain; (2) the individual's whereabouts are unknown; or (3) there is reason to suspect that the person has been encountered by an M5 partner country.

Additionally, the Federal Bureau of Investigation (FBI), DHS, and the U.K. share biometric information in relation to known or suspected terrorists (KSTs) for the purpose of national security and law enforcement. TRACS is used to record case search updates and create status reports of the findings, which are shared with the U.K. and authorized users. TRACS does not contain biometric information. The details of sharing are outlined in in the aforementioned IDENT PIA Appendix.[39]

Preventing and Combating Serious Crime

Since 2008, the United States has signed Preventing and Combating Serious Crime (PCSC) agreements with countries that participate or seek to participate in the Visa Waiver Program (VWP). The agreements formalize the sharing of biometric and biographic data for the purposes of preventing and combating serious crime. OBIM analysts use TRACS to support the PCSC data sharing activities by recording queries about individuals of interest, search results, and the

[37] The signed Memorandum of Understanding (January 2008) is between DHS and the U.K. Home Agency, formerly known as U.K. Visas, as the Authority Appointed by the Secretary of State for the Home Department and the Secretary of State for Foreign and Commonwealth Affairs of the United Kingdom of Great Britain and Northern Ireland, regarding Information Vetting and Sharing. Formerly, US-VISIT, and now OBIM, use the biographic and biometric information received from the U.K. International Group Visa Services Project, and provided by the visa applicant, to determine whether the applicant's biometrics are currently included in the IDENT list of subjects of interest. In the event of a biometric match, OBIM uses additional biographic information provided by the U.K. to support any necessary law enforcement or immigration enforcement investigations. *See* DHS/NPPD-002 DHS Automated Biometric Identification System (IDENT) Appendices, *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[38] *Id.*

[39] *Id.*

information OBIM provides in response to the queries. The details of sharing are outlined in PCSC-related PIAs and appendices attached to the aforementioned IDENT PIA Appendix.[40]

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

TRACS does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

TRACS is an information management system that helps analysts ensure data accuracy in IDENT through its function as a mechanism for supporting redress requests. Automated reports generated from information TRACS pulls from IDENT provide data accuracy, completeness, and timeliness of transactions and are stored in TRACS. Individuals can submit a redress request through DHS TRIP for a review and correction of potential inaccurate data. System owners train OBIM analysts to check redress requests and access source systems to ensure accuracy in IDENT. OBIM analysts use TRACS to support the search of the redress request, record the case findings, and document the resolution. If OBIM analysts determine IDENT data is incorrect, BSC examiners make the correction to IDENT. This also improves the data accuracy in TRACS, which receives its data from IDENT.

TRACS receives data from data owners. One of the primary functions of TRACS is to compare various data to ensure that any action taken is based on the most accurate, complete, and up-to-date data. If OBIM finds information that requires updating, OBIM reaches out to the data owner with a data correction recommendation.

For example, under the U.K. Home Office Visa Services Project, the U.K. Home Office requests additional information from OBIM if the subject of a query is on the IDENT fast matcher. OBIM analysts use IDENT information, as well as source-system information, for example from the ICE EAGLE[41] database, to research the reason the individual is an IDENT fast matcher. OBIM provides the U.K. Home Office with the additional information so they can make a determination based on accurate information. If, while reviewing the case, OBIM identifies a reason why the individual in question should be removed as a fast matcher in IDENT, OBIM will make a recommendation to the data owners. The data owner will review the recommendation, conduct a review of the source system as appropriate, and make the final determination.

[40] *See* DHS/ALL/PIA-064 Preventing and Combating Serious Crime (PCSC) Agreements - Greece and Italy, *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.
[41] *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID), *available at* https://www.dhs.gov/privacy-documents-ice.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that since the data in TRACS comes from other systems it may be incorrect and out of date.

Mitigation: This risk is partially mitigated. OBIM analysts perform certain quality checks (e.g., verifying against source system information) to ensure accuracy before sharing data. Ultimately, the responsibility is of the original data owner to ensure that the data in their systems is accurate. OBIM analysts do not only rely on previously recorded data in TRACS but check source systems to confirm the accuracy of the data for each new request.

By using IDENT's interface, Secondary Inspection Tool (SIT), OBIM analysts identify new IDENT encounters that have been added since the original match was made and edit their findings, as appropriate, which also helps to mitigate this risk. The findings provided to the recipient are accurate as of the date provided. Additionally, if a recipient notifies OBIM of a possible inaccuracy, OBIM coordinates with the data owner for resolution.

Privacy Risk: There is a risk that TRACS receives more information than necessary to accomplish its functions.

Mitigation: This risk is mitigated. TRACS receives the minimum amount of data to support its mission. For example, if a foreign partner queries IDENT and the data cannot be shared, a no match response is provided to the requestor. In such cases, OBIM analysts would not import data from IDENT to TRACS. Additionally, only a limited amount of OBIM employees and contractors have access to TRACS. Foreign partners cannot directly access the data in TRACS that the OBIM employees use for their analysis. OBIM employees only share the results of the analysis.

In a separate example, if a foreign partner query matches to an IDENT record that contains both sharable and non-sharable encounters, the non-sharable encounters are filtered out of the IDENT response. Since OBIM analysts have a need to know, all encounters (sharable and non-sharable) are imported into TRACS so OBIM can properly review the case. OBIM analysts use TRACS features to set visible flags on those encounters that should not be shared with the partner to facilitate analysis.

Privacy Risk: There is a risk of unauthorized manipulation of data within the TRACS database.

Mitigation: This risk is mitigated. OBIM limits TRACS access to OBIM users. Additionally, a large number of the fields within the database are locked from being edited or manipulated, which means OBIM analysts cannot modify the data contained in certain fields. This risk is also mitigated by TRACS audit logs that record when a record is last modified and by whom.

Privacy Risk: There is a risk that data quality will not be maintained since TRACS users have the ability to manually apply derogatory and disposition information.

Mitigation: The risk is not mitigated. OBIM cannot ensure accuracy since the information is not automatically pulled from the source system. OBIM does not coordinate with users to determine what derogatory information they are authorized to share. OBIM intends to coordinate with source system data owners to train users on how to use the newly developed HART's derogatory services in accordance with the source system mission and business rules.

Privacy Risk: There is a risk that the quality and integrity of information collected and maintained in TRACS may not be sufficient to serve the purpose of biometric and biographic matching for verification or investigation, thus potentially resulting in misidentification.

Mitigation: This risk is partially mitigated. TRACS does not contain biometric information; however, OBIM mitigates this risk by requiring fingerprints, which are unique identifiers, and basic biographic information, to establish an identity in IDENT and subsequent HART system. OBIM performs quality checks on fingerprints (e.g., determining the quality of a captured fingerprint and its suitability for matching in the future) and seeks to ensure that the data meets a minimum level of quality and completeness. OBIM conducts testing to monitor and maintain the accuracy and integrity of the biometric data.

The original data owner, whether external or internal to DHS, is responsible for ensuring the accuracy, completeness, and quality of the original data collected and submitted to OBIM. OBIM recommends that data providers follow industry-standard best practices and guidelines for biometrics.

Privacy Risk: There is a privacy risk that TRACS users may inadvertently share incorrect information.

Mitigation: This risk is mitigated. TRACS receives the minimum amount of data to support OBIM's mission. TRACS users may set filters and visual flags that identify which types of encounters should and should not be shared with the requestor, according to the terms of the relevant ISAA or other sharing requirements. These filters and flags partially eliminate the risk of inadvertent manual wrongful disclosure of information in the case summaries as well. The number of analysts accessing the system is limited. OBIM analysts are subject matter experts acting under the Component data owner authorities. OBIM analyst supervisors outline the specific sharing requirements of users based on the instructions of the data owners. Employees are instructed by standard of operating procedure and sharing agreements and are shown the usage capabilities of the system.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

OBIM uses TRACS to facilitate research necessary to respond to queries, consolidate findings, detect inconsistent records, manually share information, and coordinate with data owners. OBIM also uses TRACS for operational reporting, statistical reporting to OBIM and DHS leadership, and coordination of domestic and international data sharing with the law enforcement and international and intelligence communities.

OBIM Use

Information Sharing Coordination with Foreign Partners

OBIM uses TRACS to track and respond to data sharing inquiries from foreign governments, external agencies, and immigration agencies. For example, when the U.K. Home Office submits the fingerprints of a visa applicant to search IDENT and a match is found, the biographic information from the match is shared with and maintained in TRACS. The U.K. Home Office may request additional biographic information on the subject of the match, prompting OBIM analysts to search source system databases, compile the findings, and provide a summary to the U.K. Home Office for use in the visa adjudication. Similarly, OBIM uses TRACS to compile search results and provide case summaries for the PCSC[42] data exchange, which is done to prevent, detect, and investigate serious criminal activities.

Redress

OBIM uses TRACS to track and respond to redress requests from individuals and IDENT system users. TRACS ingests information from IDENT and other immigration and law enforcement systems to search IDENT records on individuals who have submitted redress requests for manual correction of possible mismatches. For example, if an individual has a fingerprint record incorrectly linked to another person's record, that individual may be incorrectly processed at entry to the United States. If the individual submits a redress request, OBIM analytes use TRACS to record case search results and document the resolution of the case. Redress request resolution eases the travel process for the individual the next time he or she enters the country and ensures that OBIM records are as accurate, complete, and up-to-date as possible.

Reporting Functions and Administrative Tasks

TRACS supports administrative functions, such as training, management reporting, quality control and process improvement, and system planning and analysis. For example, OBIM uses TRACS to create the OBIM DOSR, which depicts IDENT's daily transactions, including the

[42] *See* DHS/ALL/PIA-064 Preventing and Combating Serious Crime (PCSC) Agreements - Greece and Italy, *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

number of subjects processed in IDENT, the number of KST matches identified, the number of matches identified, and match rates. No PII is provided in this report.

TRACS is also used to manage the OBIM EPR. The OBIM EPR examines OBIM's performance measurements in detail and provides background, results, and projected future progress toward achieving goals for each. For example, the OBIM EPR provides statistics on OBIM's redress function (e.g., average processing time for redress cases, number of requests OBIM receives, longest time it takes to process a case). No PII is provided in this report.

Finally, TRACS records iterations of Information Bulletins that provide situational awareness to internal and external users that may have direct or indirect interest in the case. TRACS maintains, among other items, the document title, document description, date created, date it was sent to Executive Secretariat, and date approved by Executive Secretariat. Information Bulletins contain the summary of the case, the identity management services provided, and the outcome of the request if applicable. Information Bulletins do not contain any PII, besides the name of the OBIM author. For example, one Information Bulletin highlighted how OBIM fingerprint examiners were able to identify an unknown deceased individual after a bus accident by searching the fingerprints through IDENT and making a match. The Information Bulletin included a high-level summary of the event and was provided to internal and external stakeholders.

TRACS Reports Shared with DHS Components

As part of M5 data sharing agreements, certain IDENT encounters are shared with foreign partners. When a foreign partner submits prints for query, and IDENT finds a match, OBIM provides these encounters to the foreign partner when permissible. For example, when a match is made against USCIS's information by an inbound foreign partner query and shared, if permitted, USCIS is notified. OBIM analysts use TRACS to record DHS Components' notification of matches against their data from M5 countries. TRACS is then used to generate reports as needed.

External Agency Use of OBIM Reports and Case Findings Supported by, Created with, and Maintained in TRACS

The data compiled in TRACS may be used to generate reports and findings to external federal and foreign government agencies consistent with DHS policies, statutes, and ISAAs, including those entities with national security, immigration, or law enforcement responsibilities, such as:

Department of State (DOS)

Certain DOS encounters in IDENT may be shared with foreign partners under M5 information sharing agreements. When IDENT is searched using a foreign partner's submitted fingerprints, OBIM generates a report of the encounters (which may include DOS encounters) that are associated with the fingerprint match. OBIM alerts DOS that their data was matched against

an inbound foreign partner query and provides a report, generated from TRACS, of the encounters subsequently shared.

Federal Bureau of Investigation (FBI) Terrorist Screening Center (TSC)

When matches are made against FBI Terrorist Screening Center (TSC) encounter(s), OBIM sends the FBI TSC a notification of the match(es) regardless of whether or not they were shared with the foreign partner. This allows FBI TSC the opportunity to notify OBIM if the subject of the match is no longer in their database and should be removed from IDENT. In such cases, OBIM will remove the encounter. OBIM uses TRACS to generate notifications and reports to the TSC of matches to their data.

U.K. Home Office

OBIM uses TRACS to compile case summaries, which are shared with the U.K. Home Office to assist in their adjudication of visas or other travel documents according to applicable U.K. laws. This information sharing enhances the integrity of the U.S. immigration system because it augments DHS information.

Migration 5 (M5)

OBIM provides M5 countries information from TRACS in response to queries made for immigration and border management, national security and law enforcement purposes. The case information shared from TRACS supports immigration processes, including asylum, visa, and refugee determinations, as well as admissibility, among the M5 partners.

PCSC

TRACS case information may be provided to signatory countries to PCSC agreements and is used to facilitate the timely exchange of information between the partners regarding the prevention, detection, and investigation of serious criminal activities.

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. TRACS does not use technology to conduct electronic searches, queries, or analyses to discover or locate a predictive pattern or an anomaly.

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

No. TRACS users include only a limited number of OBIM employees and contractors.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that OBIM analysts may use information for purposes inconsistent with the purpose of the original collection.

Mitigation: This risk is mitigated. Only OBIM employees and contractors with a need to know have access to TRACS. TRACS has no users external to OBIM.

OBIM shares TRACS reports with authorized users for an authorized use, pursuant to ISAAs[43] or, within DHS, interconnectivity service agreements. When OBIM sends TRACS reports to a user, for example DOS, DOS only receives the DOS data that has been matched to a foreign partner query. DOS does not receive information sourced from other data owners.

In addition, OBIM disseminates information from TRACS consistent with DHS's information sharing policies and ISAAs. Information stored in TRACS may be shared with other DHS Components, as well as appropriate federal, state, local, tribal, foreign, or international government agencies, when permitted by law and DHS policies. DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, or immigration functions consistent with the routine uses set in the EBAR SORN.[44]

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.

TRACS does not provide individuals notice prior to the collection of information, as it is an information management tool used to coordinate information sharing and reporting activities with external agencies and foreign partners. This PIA and EBAR SORN provide general notice that individuals' personal information may reside in TRACS. Notice is also provided through the publication of PIAs and SORNs on the underlying systems of original collection and the information shared from those systems. If required by law or policy, DHS Components, as well as external partners that submit information to TRACS and other DHS systems, provide notice to the individual at the point of collection related to storage and retention of information, including whether it is retained initially in IDENT or eventually in HART.

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

TRACS is not the original source of the data collection. Because TRACS operates as an information management tool, individuals should consult other DHS programs' or external

[43] *See* Appendix A.
[44] DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR) System of Records, 85 FR 14955 (Mar. 16, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.

partners' PIAs[45] for specifics on opportunities to opt-out.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Individuals may not be aware that information collected directly from them (e.g., provided during an application for a benefit) may be stored in TRACS and shared with other TRACS data providers' databases.

Mitigation: This risk is partially mitigated. OBIM cannot fully mitigate this risk because OBIM is not the original collector of the information. OBIM partially mitigates this risk through publication of this PIA and other Departmental applicable SORNs. The published EBAR SORN[46] covers administrative records maintained in TRACS. It covers the Fingerprint Identification Number, Encounter Identification Number, and other transactional information owned by OBIM, and provides notice of this collection. However, because TRACS does not itself collection any information, OBIM is dependent on the source system data owners to provide notice where appropriate.

Section 5.0 Data Retention by the project

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

OBIM is currently developing the transactional record systems retention schedule. Once complete OBIM will submit to NARA for approval.

OBIM currently keeps international records for 75 years. DHS is re-evaluating the current retention policy to determine whether a new retention period or combination of retention periods is appropriate.

OBIM's current Record Schedule, DAA-0563-2013-0001,[47] covers DHS biometric and biographic records used for national security, law enforcement, immigration, and other functions consistent with DHS authorities has been approved by National Archives and Records Administration (NARA). EBR records include:

- Law Enforcement Records: Identification, investigation, apprehension, and/or removal of aliens unlawfully entering or present in the United States and facilitate legal entry of individuals into the United States, which must be destroyed or deleted 75 years after the end of the calendar year in which the data is gathered.
- Records related to the analysis of relationship patterns among individuals and organizations

[45] *See* Appendix A for a list of authorized users.
[46] DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR) System of Records, 85 FR 14955 (Mar. 16, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.
[47] https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0001_sf115.pdf.

that are indicative of violations of the customs and immigration laws including possible terrorist threats from non-obvious relationships and specific leads and law enforcement intelligence for active and new investigations. These records must be destroyed or deleted 15 years after the end of calendar year of last use of individual's data.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that TRACS data may be retained for a longer period than is necessary for the purpose for which the information was collected.

Mitigation: This risk is not currently mitigated. TRACS is an information management tool used to assist OBIM analysts in providing updates and analysis to queries from immigration and law enforcement agencies charged with national security, law enforcement, and immigration. The transactional record systems retention schedule is currently in development with OBIM and will be submitted thereafter to NARA for approval. Until this retention schedule can be approved, this risk cannot be mitigated.

Privacy Risk: There is a risk that data owners may not delete their records in a timely manner or in accordance with their respective retention schedule.

Mitigation: This risk is not currently mitigated. Data owners are responsible for deleting their information in accordance with the applicable data retention schedule, using IDENT technical services. OBIM governs retention with data owners prior to submitting information to IDENT through the Memoranda of Understanding (MOU) and other policy documentation. Although TRACS information duplicates records in IDENT, the data owner is unable to apply the proper retention requirements as they do not have access to TRACS. Until the previously discussed retention schedule can be approved, this risk cannot be mitigated.

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.

OBIM shares information in TRACS as part of normal agency operations with appropriate federal, state, local, tribal, and territorial law enforcement agencies, and foreign and international agencies for national security, law enforcement, criminal justice, immigration screening and border management, and intelligence purposes, consistent with ISAAs facilitated by the DHS Office of Strategy, Policy, and Plans (PLCY). TRACS supports information sharing coordination with non-DHS entities, such as the M5 Partners, PCSC initiative, and the U.K. Home Office Visa Services Project. As part of the U.K. Home Office Visa Services Project, OBIM searches authorized immigration and law enforcement systems and creates a case summary in TRACS, after

the foreign partner receives an IDENT response and submits a follow-up request. The case findings may include details behind adverse actions, travel history, and fast matchers. OBIM manually shares the case findings with the U.K. Home Office so they can make a determination on the individual they encountered.

Information in TRACS is also shared outside of DHS to support OBIM's redress function. For instance, if IDENT matches an M5 query to an FBI TSC record, OBIM logs the match in TRACS and shares that information with the FBI TSC to confirm whether the individual is currently in the TSC's database or, if not, that hr or she should be removed from IDENT. At the direction of the FBI TSC, OBIM removes the TSC encounter from IDENT, thus making the individual's record in IDENT reflect the most recent information.

Finally, OBIM issues reports drafted from information maintained in TRACS and shares them outside of the Department as appropriate. Reports such as Information Bulletins[48] and identity management services are shared with external stakeholders. In addition, reports that discuss IDENT's functionality, the number of IDENT's daily transactions, and the number of KST matches identified are shared with authorized internal and external stakeholders.

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

DHS/ALL-043 EBAR System of Records covers the administrative and technical records of IDENT and the successor system, HART. DHS/ALL-041 EBR System of Records governs the maintenance and use of biometrics and associated biographic information received from non-DHS entities that are not covered by existing DHS Component SORNs. DHS Component SORNs govern the function and use of the biometrics records collected by each Component. Each data owner must determine whether sharing is compatible prior to permitting the release of the information. Together, the EBAR SORN, EBR SORN, and the underlying component SORNs provide coverage for TRACS.

6.3 Does the project place limitations on re-dissemination?

External data owners sign ISAAs that govern the sharing of data retained via IDENT. TRACS pulls the biographic information from IDENT in order to create case summaries that are manually disseminated to a specific user as authorized in the respective ISAA. ISAAs may include Memoranda of Agreement (MOA), MOUs, Implementing Agreements (IA), or other formalized letters describing the purpose, use, and scope of sharing. Those agreements include limitations and restrictions on re-dissemination and third-party sharing. These limitations are discussed in Component privacy compliance documentation as referenced in Appendix A.

[48] Information Bulletins contain the summary of the case, the identity management services provided, and the outcome of the request.

DHS policy requires that DHS oversight offices, including the DHS Privacy Office, as well as the relevant Component Privacy and Security offices and Component System Owner, review and approve ISAAs, including MOUs, MOAs, and IAs.[49] DHS Component Privacy Offices, including OBIM Privacy, are required to review technologies, policies, procedures, guidelines, programs, projects, or systems (including pilot activities), whether proposed or operational, for potential privacy impacts. OBIM Privacy coordinates and communicates the results of this privacy and policy analysis to OBIM analysts to ensure proper implementation.

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

OBIM retains a general accounting of records disclosed outside of the Department. The disclosures include records that are electronic and record the date, nature, and purpose of each dissemination and disclosure, along with the agency to which the disclosure is made. TRACS information is shared manually via email. OBIM maintains a log of these disclosures in TRACS and any extract of data in Excel spreadsheets in an access-controlled secure folder.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Because of the sensitivity of certain classes of individuals' data collected by DHS Components, there is a potential risk that sensitive data may be shared with groups not authorized to receive the data.

Mitigation: This risk is partially mitigated. It is possible unauthorized sharing from TRACS may still occur without OBIM leadership or DHS Component knowledge. The main source of TRACS data is the IDENT system, which incorporates a robust filtering process based on the data owners' requirements for all information sharing. An IDENT data provider may inform OBIM of data sharing limitations. IDENT filtering capabilities ensure that data is only shared with data provider-approved agencies for approved purposes; this includes the data shared with TRACS when a match is made in IDENT. IDENT users who are authorized to receive special protected class information,[50] would receive caveat language in the comment field for protected classes, making them aware of the confidentiality provisions. OBIM is currently in the process of finalizing caveats for all classes of protected individuals.

TRACS users may set filters and visual flags that identify which types of encounters should and should not be shared with the requestor, according to the terms of the relevant ISAA. These

[49] *See* DHS Instruction 047-01-001 Privacy Policy and Compliance (July 2011), *available at* https://www.dhs.gov/privacy-policy-guidance.

[50] Special protected classes include T, U, and VAWA nonimmigrants, Asylee and Refuges, and Temporary Protected Status. These individuals receive special confidentiality through statute, regulation, or DHS policy. These confidentiality provisions generally prohibit the disclosure or use of any information about applicants for, and beneficiaries of, certain victim-based immigration benefits, including those applied for those under 8 U.S.C. sec. 1367 and other provisions.

filters and flags partially eliminate the risk of inadvertent manual distribution of non-sharable information in the case summaries as well.

Privacy Risk: There is a risk that TRACS provides foreign partners more information than is necessary for the purpose set out in the applicable ISAA.

Mitigation: This risk cannot be fully mitigated. However, foreign partners' audit and redress provisions may be used to detect improperly shared information and provide redress. Additionally, DHS PIAs[51] related to sharing with foreign partners lend additional transparency to those external partners' provisions. OBIM will also audit information sharing in TRACS annually to ensure consistency with ISAAs, data provider, and DHS policies.

TRACS uses the organizational filtering implemented in IDENT. Organizational filtering, also called Organization/Unit/Subunit (O/U/S) filtering, uses configuration settings within the IDENT system to remove information about encounters that are not permissible to share from responses to the authorized user's query. IDENT authorized users have an O/U/S account for their specific agency or organization, and their account receives information in accordance with defined filtering rules as determined by statutes, DHS policies, and ISAAs, and as approved by data owners.

Section 7.0 Redress

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

U.S. citizens, lawful permanent residents, and individuals who have records covered under the Judicial Redress Act (JRA) may file a Privacy Act request to access their information. Requesters may indicate the modality for the basis of the search. Those individuals may submit a request to OBIM Privacy: Chief Privacy Officer/Chief Freedom of Information Act Officer, U.S. Department of Homeland Security, 2707 Martin Luther King Jr. Avenue, S.E., Washington, D.C. 20528-0628.

All individuals, regardless of citizenship, may obtain access to records consistent with the Freedom of Information Act (FOIA) unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. The OBIM FOIA contact address is: Chief Privacy Officer/Chief Freedom of Information Act Officer, U.S. Department of Homeland Security, 2707 Martin Luther King Jr. Avenue, S.E., Washington, D.C. 20528-0628. Requests for information are evaluated to ensure that any release of information is lawful and does not disclose information that would cause a clearly unwarranted invasion of personal privacy or that would disclose techniques and/or procedures for law enforcement

[51] *See* Appendix A.

investigations or prosecutions.

Certain information may be exempt from individual access because access to the data in TRACS could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, or to the existence of the investigation, and could reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, or to avoid detection or apprehension. DHS will review and comply appropriately with information requests on a case-by-case basis. Access may be limited though pursuant to exemptions asserted under the Privacy Act's 5 U.S.C. secs. 552a(j)(2) and (k)(2) provisions for the TRACS system.

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

U.S. citizens and lawful permanent residents, as well as other covered persons with records covered by the JRA, may seek to amend inaccurate records by filing a Privacy Act amendment request under the Privacy Act. Those individuals covered under by the JRA or Privacy Act may direct all requests to contest or amend information to Chief Privacy Officer/Chief Freedom of Information Act Officer, U.S. Department of Homeland Security, 2707 Martin Luther King Jr. Avenue, S.E., Washington, D.C. 20528-0628. Individuals must state clearly and concisely in the redress request the information being contested, the reason for contesting it, the proposed amendment.

If an individual is dissatisfied with the response to his or her redress access or amendment request, that individual may appeal an adverse determination denying such request in any respect to the DHS Office of the General Counsel or its designee, U.S. Department of Homeland Security, Washington, D.C. 20528, pursuant to 6 CFR Part 5, Subpart B. Contact information is available here: https://www.dhs.gov/office-general-counsel. The DHS Chief Privacy Officer can be contacted at:

Chief Privacy Officer/Chief Freedom of Information Act Officer
U.S. Department of Homeland Security
2707 Martin Luther King Jr. Avenue, SE
Washington, D.C. 20528
Phone: 202-343-1743 or 866-431-0486
Fax: 202-343-4011
E-mail: foia@hq.dhs.gov

As with access requests, amendments may be limited pursuant to applicable Privacy Act exemptions asserted under 5 USC secs. 552a(j)(2) and (k)(2) for the TRACS system.

Additionally, travelers who wish to file for redress can complete an online application

through the DHS Traveler Redress Inquiry Program (DHS TRIP)[52] at https://trip.dhs.gov, or mail or email a completed copy of DHS Form 591, Travel Inquiry Form (TIF). For more information about the types of services DHS TRIP can provide, please visit https://www.dhs.gov/step-1-should-i-use-dhs-trip.

Completing the form online saves processing time and helps prevent data entry errors. After an individual submits a redress form, DHS TRIP will send a notification receipt to the individual. DHS TRIP will review the redress form and will determine which component/agency will respond most effectively to the submission. When a redress request is related to records maintained in IDENT/HART, DHS TRIP will coordinate with OBIM. OBIM will then review the individual's records and correct the information, if appropriate. DHS TRIP will notify the individual of the resolution of that request.

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

Individuals are advised of the procedures for correcting their information in this PIA, or by contacting the OBIM Privacy, U.S. Department of Homeland Security, 2707 Martin Luther King Jr. Avenue, S.E., Washington, D.C. 20528-0628. The redress procedures are established and operated by DHS through DHS TRIP, which can be accessed at www.dhs.gov/trip.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals or organizations will be unable to correct inaccurate or erroneous information about themselves in TRACS.

Mitigation: This risk is not fully mitigated. OBIM uses TRACS as an information management tool that contains PII from various other databases within DHS Components and external agencies, via IDENT. Because TRACS is not a source system and copies data from other systems of origin, the data must be corrected in the system of origin in order for OBIM to correct the information in TRACS. As a result, OBIM's ability to itself correct individuals' data in TRACS is limited. Individuals only have the option to access and correct his or her PII directly from the agencies or organizations that originally collected it.

For travelers, DHS TRIP provides a redress process through a website that facilitates the submission and processing of redress requests. Any individual can request access to or correction of his or her PII regardless of nationality or country of residence. This process has been described in the DHS TRIP PIA and information is available in multiple places on DHS's public website.

Alternatively, any person may submit a redress request to have a record corrected by

[52] DHS/ALL/PIA-002 DHS Traveler Redress Inquiry Program (TRIP), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

contacting OBIM FOIA at: Chief Privacy Officer/Chief Freedom of Information Act Officer, U.S. Department of Homeland Security, 2707 Martin Luther King Jr. Avenue, S.E., Washington, D.C. 20528-0628.

However, all these mechanisms still require OBIM analysts to ensure they are accurately pulling information from source systems, via IDENT, during each case to ensure any corrected information is accurately reflected in TRACS.

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?

Existing ISAAs, such as MOUs, cover TRACS data sharing activities in which the signatories have agreed to data sharing per specific conditions. A technical safeguard that ensures TRACS information is used in accordance with established practices is that only the information that directly relates to the individual case is contained in TRACS. When information is imported from IDENT to TRACS, there is a flag that indicates if the record belongs to a special protected class, so that OBIM analysts are aware of filtering rules when sharing this data with foreign partners. OBIM is working to ensure that caveat language in the comment data field of all special protected classes records in IDENT indicate that special protected class confidentiality provisions apply.

TRACS complies with the requirements of DHS information technology security policy, particularly the DHS Information Technology (IT) Security Program Handbook for Sensitive Systems (Attachment A to DHS Management Directive 4300.1). This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules. OBIM Security conducts an annual TRACS self-assessment where one third of the security controls are assessed each year to ensure that it complies with these security requirements.

TRACS provides audit trail capabilities in order to monitor, log, and analyze system transactions, as well as actions and system accesses of authorized TRACS stakeholders.

As TRACS contains data from a variety of sources, collected for a variety of uses, it is necessary to institute controls so that only those individuals with a need to know are able to access that data. Misuse of the data in TRACS is mitigated by requiring that TRACS users conform to appropriate security and privacy policies, follow established rules of behavior, and be adequately trained regarding the security of their systems. Also, a periodic assessment of physical, technical, and administrative controls is performed to enhance accountability and data integrity.

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

DHS provides comprehensive privacy training that all DHS personnel are required to participate in within the first 30 days of their assigned entry on duty. This follows the high-level DHS overview privacy training as part of new-employee orientation. Employees and contractors supporting DHS systems, have limited access based on their roles and need to know, and they are trained in the handling of personal information and PII for mission- and non-mission-related data (e.g., human capital and employment data). In addition, all DHS employees are required to complete annual Privacy Awareness Training. All system users must complete annual refresher training to retain system access. When DHS personnel complete the training, it is recorded in their file online.

DHS users of DHS/OBIM systems, and all employees and contractors supporting its systems, have limited access based on their roles and need to know, and they are trained in the handling of personal information.

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

The minimum requirements for access to OBIM systems, including TRACS, are documented in the ISAAs between and among DHS and specific stakeholders, and in security, technical, and business documentation. In particular, individuals with TRACS system access must hold a security clearance, must have a need to know the information based on their job responsibilities, and must successfully complete security and privacy training.

Some contractors may have access to TRACS data. The extent of access varies based on the need to fulfill the requirements of the employment contract under appropriate nondisclosure and use limitations, in addition to requirements enumerated in Section 8.1 of this document. OBIM ensures that all employees and contractors supporting its systems have limited access based on their roles and that they are trained in the handling of PII.

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?

DHS policy requires that ISAAs, including MOUs, MOAs, and IAs, are reviewed and approved by DHS oversight offices, including the DHS Privacy Office, as well as the relevant Component Privacy and Security Offices and Component System Owner.[53] DHS Component

[53] *See* DHS Instruction 047-01-001 Privacy Policy and Compliance (July 2011), *available at*

Privacy Offices, including OBIM Privacy, are required to review technologies, policies, procedures, guidelines, programs, projects, or systems (including pilot activities), whether proposed or operational, for potential privacy impacts, and advise DHS leadership and DHS Components on implementing corresponding privacy protections.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk: There is a risk of unauthorized access and use of data maintained in TRACS since there is a lack of defined user roles. OBIM analysts have access to each application within TRACS (e.g., redress, reporting, M5, PCSC), even if they are not the primary analyst for that project.

Mitigation: This risk is not fully mitigated. TRACS does not have user-based access controls. OBIM attempts to mitigate this risk by limiting the number of TRACS users within OBIM and only OBIM employees and contractors have access to TRACS. However, because of the configuration of TRACS and lack of user roles based on function or responsibility, each user has access to all data in TRACS.

Responsible Officials

Dwight Greene
Section Chief - Privacy and Policy
DHS/OBIM

Kenneth Gantt
Assistant Director
DHS/OBIM
(202) 298-5200

Approval Signature

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

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

https://www.dhs.gov/privacy-policy-guidance.

Appendix A: Privacy Compliance Documentation

U.S. Customs and Border Protection (CBP)

CBP PIAs: https://www.dhs.gov/privacy-documents-us-customs-and-border-protection

- DHS/CBP/PIA-002 Global Enrollment System (GES);
- DHS/CBP/PIA-006 Automated Targeting System (ATS);
- DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS);
- DHS/CBP/PIA-012 CBP Portal (e3) to EID/IDENT;
- DHS/CBP/PIA-021 TECS System: Platform;
- DHS/CBP/PIA–024 Arrival and Departure Information System;
- DHS/CBP/PIA-026 Biometric Exit Mobile Program;
- DHS/CBP/PIA-051 Automated Passport Control (APC) and Mobile Passport Control (MPC); and
- DHS/CBP/PIA-056 Traveler Verification Service.

CBP SORNs: https://www.dhs.gov/system-records-notices-sorns.

- DHS/CBP-002 Trusted and Registered Traveler Programs, 85 FR 14214 (Mar. 11, 20120);
- DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012);
- DHS/CBP-007 Border Crossing Information (BCI), 81 FR 89957 (Dec. 13, 2016);
- DHS/CBP-010 Persons Engaged in International Trade in Customs and Border Protection Licensed/Regulated Activities, 73 FR 77753 (Dec. 19, 2008);
- DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (Dec. 19, 2008);
- DHS/CBP-021 Arrival and Departure Information System (ADIS), 80 FR 72081 (Nov. 18, 2015); and
- DHS/CBP-023 Border Patrol Enforcement Records System of Records (BPER), 81 FR 72601 (Oct. 20, 2016).

U.S. Immigration and Customs Enforcement (ICE)

ICE PIAs: https://www.dhs.gov/privacy-documents-ice

- DHS/ICE/PIA-001 Student and Exchange Visitor Program (SEVP);
- DHS/ICE/PIA-003 electronic Travel Document System;
- DHS/ICE/PIA-009 Fugitive Case Management System (FCMS);
- DHS/ICE/PIA-011 Visa Security Program Tracking System;
- DHS/ICE/PIA-015 Enforcement Integrated Database (EID);
- DHS/ICE/PIA-020 Alien Criminal Response Information Management System (ACRIMe);
- DHS/ICE/PIA-049 ICE Parole and Law Enforcement Programs Unit Case Management Systems;
- Forthcoming Biometric Identification Transnational Migration Alert Program (BITMAP) PIA.

ICE SORNs: https://www.dhs.gov/system-records-notices-sorns

- DHS/ICE 001 Student and Exchange Visitor Information System, 75 FR 412 (Jan. 5, 2010);
- DHS/ICE-006 Intelligence Records System (IIRS), 75 FR 9233 (March 1, 2010);
- DHS/ICE-007 Criminal History and Immigration Verification (CHIVe) System of Records, 83 FR 20844 (May 8, 2015);
- DHS/ICE-009 External Investigations, 75 FR 404 (Jan. 5, 2010);
- DHS/ICE-010 Confidential and Other Sources of Information, 78 FR 7798 (Feb. 4, 2013);
- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (Oct. 19, 2016); and
- DHS/ICE-014 Homeland Security Investigations Forensic Laboratory, 81 FR 45523 (July 14, 2016).

U.S. Coast Guard (USCG)

USCG PIAs: https://www.dhs.gov/privacy-documents-us-coast-guard

- DHS/USCG/PIA-002 USCG "Biometrics at Sea" System (BASS).

USCG SORNs: https://www.dhs.gov/system-records-notices-sorns

- DHS/USCG-031 USCG Law Enforcement (ULE) System of Records, 81 FR 88697 (Dec. 8, 2016).

U.S. Citizenship and Immigration Services (USCIS)

USCIS PIAs**:** https://www.dhs.gov/uscis-pias-and-sorns.

- DHS/USCIS/PIA-007 Domestically Filed Intercountry Adoptions Applications and Petitions;
- DHS/USCIS/PIA-008 Enterprise Service Bus 2 (ESB 2);
- DHS/USCIS/PIA-016 Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems;
- DHS/ALL/PIA-027 USCIS Asylum Division;
- DHS/USCIS/PIA-045 Deferred Action for Childhood Arrivals (DACA);
- DHS/USCIS/PIA-048 USCIS International Biometric Processing Services;
- DHS/USCIS/PIA-056 USCIS Electronic Immigration System (USCIS ELIS);
- DHS/USCIS/PIA-060 Customer Profile Management Service (CPMS); and
- DHS/USCIS/PIA-068 Refugee Case Processing and Security Vetting.

USCIS SORNs: https://www.dhs.gov/system-records-notices-sorns.

- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017);
- DHS/USCIS-005 Inter-Country Adoptions Security, 81 FR 78614 (Nov. 8, 2016);
- DHS/USCIS-007 Benefits Information System, 84 FR 54622 (Oct. 10, 2019);
- DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (Nov. 30, 2015);
- DHS/USCIS–017 Refugee Case Processing and Security Screening Information System of Records, 81 FR 72075 (Oct. 19, 2016); and
- DHS/USCIS-018 Immigration Biometric and Background Check, 83 FR 36950 (July 31, 2018).

Transportation Security Administration (TSA)

TSA PIAs: https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa

- DHS/TSA/PIA-012 Transportation Worker Identification Credential (TWIC) Program;

- DHS/TSA/PIA-020 Security Threat Assessment for Airport Badge and Credential Holders;
- DHS/TSA/PIA-022 Maryland Three (MD-3) Airports;
- DHS/TSA/PIA-026 Alien Flight Student Program;
- DHS/TSA/PIA-041 TSA Pre-Check Application Program; and
- DHS/TSA/PIA-046 TSA OIA Technology Infrastructure Modernization Program.

TSA SORNs: https://www.dhs.gov/system-records-notices-sorns

- DHS/TSA-001 Transportation Security Enforcement Record System, 83 FR 43888 (Aug. 28, 2018);
- DHS/TSA 002 Transportation Security Threat Assessment System, 79 FR 46862 (Aug. 11, 2014); and
- DHS/TSA-021 TSA Pre✓™ Applications Program System of Record, 78 FR 55274 (Sept. 10, 2013).

Office of the Chief Security Officer (OCSO)

OCSO PIAs: https://www.dhs.gov/privacy-documents-department-wide-programs

- DHS/ALL/PIA-014 Personal Identity Verification/Identity Management System (PIV/IDMS); and
- DHS/ALL/PIA-038 Integrated Security Management System (ISMS).

OCSO SORNs: https://www.dhs.gov/system-records-notices-sorns

- DHS/ALL-023 Personnel Security Management System of Records, 75 FR 8088 (Feb. 23, 2010); and
- DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, 74 FR 30301 (June 25, 2009).

Federal Emergency Management Agency (FEMA)

FEMA PIAs: https://www.dhs.gov/privacy-documents-fema

- DHS/FEMA/PIA-034 Electronic Fingerprint System.

FEMA SORNs: https://www.dhs.gov/system-records-notices-sorns

- DHS/ALL-023 Personnel Security Management System of Records, 75 FR 8088 (Feb. 23, 2010); and

- DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, 74 FR 30301 (June 25, 2009).

Department of State (DOS)

- STATE-26 Passport Records, 76 FR 34966 (July 6, 2011);
- STATE-36, Security Records, 83 FR 28058 (June 15, 2018); and
- STATE-39 Visa Records, 83 FR 28062 (June 15, 2018).

Department of Justice (DOJ) and state / local / tribal / territorial law enforcement, federal, state, local investigative agencies, and

- JUSTICE/INTERPOL-001 INTERPOL-United States National Central Bureau (USNCB) Records System, 75 FR 27821 (May 18, 2010) [Note: records shared with DHS include: law enforcement, intelligence, and national security records];
- JUSTICE/DOJ-005 Nationwide Joint Automated Booking System, 72 FR 3410 (Jan. 25, 2007), 71 FR 52821 (Sept. 7, 2006); and
- JUSTICE/FBI-009 Next Generation Identification (NGI) System of Records, 84 FR 54182 (Oct. 9, 2019).

Department of Defense (DoD)

- A0025-2 SAIS DoD Defense Biometric Services, 74 FR 48237 (Sept. 22, 2009); and
- A0025-2 PMG (DFBA) DoD Defense Biometric Identification Records System, 80 FR 8292 (Feb. 17, 2015).

Office of Strategy, Policy, and Plans (PLCY), Program Manager for information sharing with international partners, including Migration 5 partners Canada, New Zealand, Australia, and the United Kingdom. DHS also shares information with Greece and Mexico.

PIAs: https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim and https://www.dhs.gov/privacy-documents-department-wide-programs

- DHS/OBIM/PIA-001 Automated Biometric Identification System (IDENT)
  - Canada – IDENT Appendices
  - New Zealand - IDENT Appendices
  - Australia - IDENT Appendices
  - United Kingdom - IDENT Appendices
  - Mexico - IDENT Appendices

- DHS/ALL/PIA-064 Preventing and Combating Serious Crime (PCSC) Agreements - Greece and Italy