



Privacy Impact Assessment
for

LeadTrac System

DHS/ICE/PIA-044

July 22, 2016

Contact Point

Peter T. Edge

Executive Associate Director

Homeland Security Investigations

U.S. Immigration & Customs Enforcement

(202) 732-5100

Reviewing Official

Jonathan R. Cantor

Acting Chief Privacy Officer

Department of Homeland Security

(202) 343-1717



Abstract

LeadTrac is a database owned by the U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Counterterrorism and Criminal Exploitation Unit (CTCEU). The function of LeadTrac is to vet and manage leads pertaining to visitors in the United States who are suspected of overstaying their period of admission or otherwise violating the terms of their admission, as well as organizations suspected of immigration violations. CTCEU and the Overstay Analysis Unit conduct research and enrich the leads in LeadTrac and, when appropriate, refer them to ICE field offices for investigation and enforcement action. LeadTrac's structure supports a subject-centered data model, ensuring multiple leads about a single subject are linked within the system. This Privacy Impact Assessment describes how the LeadTrac system collects and uses Personally Identifiable Information.¹

Overview

U.S. Immigration and Customs Enforcement (ICE) is responsible for identifying, investigating, and taking enforcement action against foreign students, exchange visitors, and other non-immigrant visitors to the United States who overstay their period of admission or otherwise violate the terms of their visa, immigrant, or non-immigrant status (hereafter "status violators"). ICE is also responsible for ensuring that certain organizations that facilitate the entry of non-immigrant students and exchange visitors comply with applicable federal laws and regulations. These organizations include schools and universities that admit non-immigrant students and entities that sponsor exchange visitor programs.

CTCEU and the Overstay Analysis Unit (OAU) reside within the National Security Investigations Division (NSID) of ICE Homeland Security Investigations (HSI). CTCEU and OAU personnel (hereafter referred to collectively as "NSID personnel" or in their roles as analysts or reviewers) query a variety of Department of Homeland Security (DHS) and non-DHS information systems for information on subjects, and enter their findings into LeadTrac to build a lead – a unified picture of a subject's criminal and immigration-related activities. Using this assembled information, NSID personnel determine which individuals or organizations warrant additional investigation as possible status violators or fraudulently operated institutions, and request that the appropriate ICE field offices initiate investigations. Using LeadTrac, personnel also prioritize leads on suspected status violators to allow investigators to focus first on individuals who present threats to national security and public safety, or are otherwise a priority under DHS and ICE enforcement policies.

¹ This document is a replacement of the original DHS/ICE-044 LeadTrac PIA, which was published on October 31, 2015. CTCEU chose not to ingest the Terrorist Screening Database (TSDB) dataset into the LeadTrac system, so the language in section 2.2 referencing that dataset has been removed. An explanatory footnote has been added to Question 2.2 as well.



LeadTrac contains the Personally Identifiable Information (PII) of suspected status violators and other individuals who may be material to a lead (e.g., family members and associates of a subject, employers, designated school officials (DSOs)). Some of these individuals may be lawful permanent residents (LPRs) or U.S. citizens. Each individual whose information is contained in LeadTrac is assigned a unique identifier to support cross-referencing between leads.

The specific PII in any LeadTrac record varies depending upon what information the source records contain. PII contained in LeadTrac records on individuals may include, but is not limited to: name, date of birth, gender, country of birth/citizenship, identifying document information (e.g., passport, visa, and driver's license), addresses, border crossing information, criminal history information, and immigration benefit information. LeadTrac is not the original source of any PII. All PII is either imported from other DHS systems or manually entered into the system by NSID personnel who have obtained the information from other DHS and non-DHS sources. All information input into a lead is tagged to identify the originating source(s).

Lead Generation

Leads in LeadTrac are initially generated in three ways: 1) NSID personnel manually initiate leads based on information from a variety of sources, including the HSI Tip Line, ICE field offices, and information that NSID personnel encounter while working up other leads; 2) LeadTrac imports multiple leads in bulk (e.g., via data extracts/spreadsheets) on an ad hoc basis that are generated from the HSI tip line, ICE field offices, and other law enforcement agencies; and 3) LeadTrac imports leads from the U.S. Customs and Border Protection (CBP) Automated Targeting System-Passenger (ATS-P).²

To manually initiate a lead, NSID personnel input basic information about a subject into LeadTrac and query the system for a match on that subject. If a record for that individual or organization already exists, personnel link the records within the system to reduce duplication of effort and ensure investigators have a comprehensive picture of a single subject's activities. At present, all leads pertaining to organizations are manually initiated.

Ad hoc imports allow multiple leads to be initiated in LeadTrac at the same time. Data is formatted and standardized so the information can be ingested into the system. The sources of the information in ad hoc imports may be the HSI Tip Line, ICE field offices, or other law enforcement agencies.

Leads imported from ATS-P originate from CBP's Arrival and Departure Information System (ADIS).³ ADIS is responsible for tracking the arrival and departure of non-United States

² For reference, the PIA for ATS, which includes ATS-P may be found here: DHS/CBP/PIA-006 Automated Targeting System (ATS) (includes ATS-P):

http://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_ats_updated_fr_0.pdf

³ DHS/CBP/PIA-024(a) Arrival and Departure Information System (ADIS): <http://www.dhs.gov/publication/arrival-and-departure-information-system>.



Citizen travelers. It contains information about aliens who have applied for admission, entered, or departed the United States, including biographical information, visa information, and photos of the individuals. In addition to its unique arrival and departure-related data, ADIS receives data from ICE's Student and Exchange Visitor Information System (SEVIS).⁴ ADIS generates leads by matching visa timelines with arrival and departure data to identify overstays, and sends those leads to ATS-P. ATS-P then enriches the leads based on supporting data available in CBP's Automated Targeting System (ATS), develops priorities based on associated risk patterns, and passes a prioritized list to LeadTrac.

For imported leads, LeadTrac employs matching logic that uses biographical information such as name, date of birth, and identifying numbers to compare existing records in LeadTrac against any new records being imported. If the system identifies a new lead as pertaining to an individual with an existing record in LeadTrac, the new lead will be associated with that individual. This prevents LeadTrac from containing multiple open records related to the same individual, reduces duplication of research and review efforts within CTCEU and OAU, and helps to ensure the accuracy of data pertaining to individuals.

LeadTrac also receives updated information directly from ADIS on leads previously imported into LeadTrac from ATS-P, which ensures LeadTrac has the most current information possible on its subjects. This includes departures and subsequent arrivals, as well as other information pertaining to an individual's immigration status. When LeadTrac receives updates from ADIS that are no longer necessary (e.g., because there has been a final disposition on the lead in LeadTrac), LeadTrac sends an indicator to ADIS that information on the individual in question should no longer be transmitted. Additionally, LeadTrac proactively transmits relevant data to ADIS to assist that system in ensuring its records are accurate (e.g., when NSID personnel confirm that a previously identified subject is deceased).

Lead Workup

After leads are initiated in LeadTrac, the system automatically prioritizes them based on programming that reflects HSI's mission needs. When NSID personnel receive leads for workup, they conduct additional research to determine the subject's immigration status and current location in the United States. Personnel search and retrieve additional information from sources outside LeadTrac and manually input any relevant data into LeadTrac. They may search a variety of governmental databases including: ATS Hotlist/Federated Query, Advance Passenger Information System (APIS), Department of State (DoS) Consular Consolidated Database (CCD), Enforcement Integrated Database (EID), Central Index System (CIS), Computer Linked Application Information Management System (CLAIMS 3), Department of Justice's Executive Office for Immigration Review (DOJ EOIR), Automated Biometric Identification System (IDENT), ADIS,

⁴ DHS/ICE/PIA-001(a) Student and Exchange Visitor Information System (SEVIS): http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_sevis.pdf.



and SEVIS.⁵ Personnel may also use commercial data provider services to retrieve publicly available information, and independently search and retrieve publicly available information from the internet.

Viable Investigative Leads

A lead is viable when the subject is a suspected status violator and is believed to have a valid U.S. address, or when an organization is suspected of committing an immigration violation, such as when visitors in the United States overstay their period of admission or otherwise violated the terms of their admission. Secondary reviewers confirm whether leads are viable and determine based on internal prioritization criteria whether to refer leads to the appropriate ICE field offices for action. NSID personnel refer leads to the field by inputting data from LeadTrac into HSI's case management system⁶ and then monitor the results of the field office investigation.

Nonviable Investigative Leads

Nonviable leads are those in which a violation is suspected but ICE deems the leads not actionable. In LeadTrac, nonviable leads may be closed or pending, depending on the findings and review by NSID personnel. A nonviable lead is closed if the subject of the lead is found to be no longer in violation of U.S. immigration law or is no longer present in the United States. Nonviable pending leads are periodically updated with new information, which may result in those leads being closed or determined viable and referred to the field for action.

Disposition

⁵ For reference, the PIAs for these systems may be found at the locations below:

- DHS/CBP/PIA-006 Automated Targeting System (ATS) (includes ATS Hotlist/Federated Query functionality): http://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_ats_updated_fr_0.pdf
- DHS/CBP/PIA-001 Advance Passenger Information System (APIS): http://www.dhs.gov/sites/default/files/publications/privacy_pia_cbpapis_0.pdf
- DoS Consular Consolidated Database PIA: https://foia.state.gov/docs/PIA/ConsularConsolidatedDatabase_CCD.pdf
- DHS/ICE/PIA-015 Enforcement Integrated Database (EID): http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_eid.pdf
- DHS/USCIS/PIA-009 Central Index System: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_cis.pdf
- DHS/USCIS/PIA-016 Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3): http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_cis.pdf
- DOJ Executive Office for Immigration Review PIA: http://www.justice.gov/sites/default/files/opcl/docs/eoir_pia.pdf
- DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT): <http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf>
- DHS/CBP/PIA-024(a) Arrival and Departure Information System (ADIS): <http://www.dhs.gov/publication/arrival-and-departure-information-system>
- DHS/ICE/PIA-001(a) Student and Exchange Visitor Information System (SEVIS): http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_sevis.pdf

⁶ See DHS/ICE/PIA-045 ICE Investigative Case Management (ICM), available at www.dhs.gov/privacy.



NSID analysts submit worked-up leads to secondary reviewers, who may make updates or return the leads to the analysts for changes. Once a lead passes secondary review, nonviable leads are closed or set to pending, and viable leads are either sent to field offices for investigation or held and monitored by NSID personnel. Leads that are not closed remain in the backlog in the event additional information is obtained. Leads that do not meet the priority criteria for investigation by HSI are extracted from LeadTrac on a weekly basis and emailed to Enforcement and Removal Operations (ERO) for review and consideration for enforcement action.

Cross-Agency Efforts

The CTCEU also plays a key role in cross-agency efforts involved in identifying and apprehending suspected status violators. These efforts may involve federal, state, local, and tribal law enforcement partners, as well as other federal agencies. Current efforts are detailed in the appendices to this PIA. In each of these efforts, the CTCEU performs its standard LeadTrac vetting process to determine if a lead is viable based on the requirements of the program. LeadTrac is used to consolidate information in one location and evaluate it for validity, and generate the documentation on which field personnel can base an investigation. Viable leads discovered as a result of these projects are then forwarded to ICE agents in the field, using the standard LeadTrac process described above. LeadTrac also contains historical data from previous cross-agency efforts that are now inactive.⁷ These datasets are maintained in LeadTrac and are searched and referenced during the lead initiation and work-up processes to identify and link previous encounters with subjects identified in new leads.

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?

ICE has been authorized to collect information in LeadTrac by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law 104-208; the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106-215; the Visa Waiver Permanent Program Act of 2000 (VWPPA), Public Law 106-396; The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (U.S.A. PATRIOT Act) of 2001, Public Law 107-56; the Enhanced Border Security and Visa Entry Reform Act (Border Security Act), Public Law 107-173; and the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53.

⁷ These efforts supported partnerships with other federal agencies to identify overstays fitting specific criteria, such as individuals who entered the country using lost or stolen passports, individuals who used fraud to obtain immigration benefits, and individuals who sponsored a known or suspected terrorist for immigration benefits. Data from these efforts are consistent with the categories of data described throughout this PIA and pertain to suspected status violators and their associates.



In addition to those mentioned above, relevant authorities include: the Aviation and Transportation Security Act of 2001 (ATSA), Public Law 107-71; the Trade Act of 2002, Public Law 107-210; the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law 108-458; the Security and Accountability for Every Port Act of 2006 (SAFE Port Act), Public Law 109-347; 8 U.S.C. § 1103 (authorizing the Secretary of Homeland Security to control immigration-related records); 8 U.S.C. § 1225(d)(3) (granting authority to take and consider evidence of an alien's privilege to enter or reside in the United States); 8 U.S.C. § 1324(b)(3) (immigration-related records may be evidence in human smuggling cases); 8 U.S.C. § 1357(a) (powers of Immigration Officers); 8 U.S.C. § 1360(b) (granting authority to establish central files to include any information kept by any department or agency as to the identity and location of aliens); 19 U.S.C. § 1 (establishment of the Customs Service); 19 U.S.C. § 1509 (granting authority to take and consider evidence relating to Customs Duties); and 8 U.S.C. § 1302 (providing for registration of aliens in the United States); 8 U.S.C. § 1303 (regarding registration of special groups); 8 U.S.C. § 1304 (regarding forms for registration and fingerprinting).

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

Information in LeadTrac is covered by the DHS/ICE-009 External Investigations SORN.⁸ ICE is publishing a new LeadTrac SORN to cover this information concurrent with this PIA.

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

Yes, LeadTrac has a system security plan in place. On August 10, 2015, LeadTrac was granted a 36-month Authority to Operate (ATO) by the ICE Office of the Chief Information Officer. The ATO approval process entailed a review of LeadTrac's documentation and a Security Controls Assessment.

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

Yes. Under the NARA-approved records retention schedule for LeadTrac, records must be retained until 75 years after the end of the fiscal year in which the cases to which those records relate are closed. However, because LeadTrac records only contain copies of data from other sources, ICE intends to request NARA approval to retain LeadTrac records for 25 years from the date the record was created. Under this schedule, records would be kept as active in LeadTrac for 20 years, and archived for an additional five-year period. After the 25-year period, the information would be destroyed or, if deemed necessary, retained further under a reset retention schedule.

⁸ DHS/ICE-009 External Investigations SORN: <https://insight.ice.dhs.gov/mgt/oop/Documents/pdf/sorn-dhs-ice-009-ext-inv.pdf>



Additionally, ICE would be able to archive records early when appropriate (e.g., death of subject, subsequent naturalization).

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.

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

Section 2.0 Characterization of the Information

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

LeadTrac contains the following information in subject records pertaining to suspected status violators:

Biographical and other identifying information: name, date of birth, country of birth, country of citizenship, gender, last known address, contact information, known aliases, SEVIS user ID (when applicable), naturalization date (when applicable), visa issuance and revocation data, border immigration and naturalization data, and identifying numbers, such as Social Security numbers and driver's license numbers. Information in this category may pertain to suspected status violators and individuals who are material to leads (e.g., dependents and other family members, associates, DSOs, school owners). Individuals who are material to leads may be U.S. citizens or LPRs.

Travel-related information: Passport and visa information, and other information related to entry and exit of the United States.

Other: Financial information; vehicle information; data related to immigration benefit applications filed with U.S. government agencies; data related to matriculation at a U.S. college or university; employment data; civil litigation and/or criminal history information; and investigative information from other DHS and non-DHS systems.

LeadTrac also includes records on organizations: Leads pertain to specific schools or universities that are being vetted by CTCEU and entities that sponsor exchange visitor programs. Other records on organizations pertain to businesses, non-profit entities, and other organizations that may be affiliated with the subject of a lead. As with individuals, every organization is assigned a unique identifier to support cross-referencing of leads within LeadTrac. The data contained in organization subject records may include: entity name, location, and contact information; website



addresses; and biographical and other identifying information of individuals who are material to a lead.

Information specific to schools may include: school code; SEVIS certification date; accreditation information; school operating authority; school type; information on science, technology, engineering, and mathematics (STEM) programs; the non-profit/for-profit status of the school; admission requirements; average annual enrollment; whether or not the school has any J-1 visa programs; and aggregated/statistical (i.e., non-PII) student information. Aggregated/statistical student information may include data such as the number of student records, the ratio of foreign to non-foreign students, and the number of non-immigrant students with dependent visas.

In addition to the above categories of information, LeadTrac contains miscellaneous types of information from a variety of sources that is received or manually input as part of the lead work-up process. This includes, but is not limited to INTERPOL notices, information on inbound and outbound cargo, and lost and stolen passport data.

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

LeadTrac is a database of consolidated information collected from a variety of Government databases and other sources. The system does not directly collect information from individuals or organizations.⁹

ATS-P and ADIS: LeadTrac imports data from both ATS-P and ADIS. The ATS-P imports consist of new leads that originate from ADIS and SEVIS data. This data is enriched by the ATS-P system and then sent to LeadTrac. The ADIS imports consist of updated arrival and departure information on subjects previously identified in leads sent from ATS-P. To ensure LeadTrac is only receiving relevant information, the system sends an indicator to ADIS when a lead has been closed or when there are other circumstances rendering updated information on a previously identified lead unnecessary. The LeadTrac system also proactively transmits data to ADIS to assist that system in ensuring its records are accurate. For example, when NSID personnel confirm that a previously identified subject is deceased or has been removed from the country, LeadTrac will provide that information to ADIS.

⁹ The legacy LeadTrac system contained a dataset from the Terrorist Screening Database (TSDB). The TSDB program for which this information was collected and analyzed in legacy LeadTrac is no longer active, therefore ICE determined there was no operational need for the data to be migrated to the new LeadTrac system described in this PIA. The TSDB project data is being maintained in an archive form outside of this system. Once the record retention period is reached, the dataset will be destroyed.



Extracts are received from ATS-P daily and from ADIS weekly. As part of the fully automated integration among Government databases and LeadTrac, the daily data extracts are transmitted via secure transmission to a LeadTrac administrator on the DHS network.

National Security Entry-Exit Registration System (NSEERS): LeadTrac contains a subset of the data that DHS collected under the former NSEERS program. This program, active from 2002 until 2011, required non-immigrant nationals or citizens of designated countries to comply with special registration procedures when entering or exiting the United States. While the program was active, CTCEU routinely identified and extracted a list of subjects that failed to comply with the terms of NSEERS. This dataset is maintained in LeadTrac and is searched and referenced during the lead initiation and work-up processes to identify and link previous encounters with subjects identified in new leads.

ATS Hotlist/Federated Query Service: LeadTrac uses this federated search service to vet leads. Currently, NSID personnel manually enter queries into ATS Hotlist to find information on subjects who are possible status violators. Relevant information is then selected, copied, and pasted into the LeadTrac record. CTCEU is developing functionality within the LeadTrac system to support an automatic search process that will trigger toward the beginning of the lifecycle of the lead. The program expects this functionality to be available in 2016.

The ATS Hotlist/Federated Query Service may retrieve data from the sources listed below. In addition to the unique data elements described for each system, all physical address information found using this search service is entered into LeadTrac along with the dates for which the information was valid.

- ***CBP's databases TECS, APIS, Electronic System for Travel Authorization, and ATS:*** Information input into LeadTrac may include biographical, visa, arrival/departures, case information for HSI criminal investigations, and other derogatory information; pre-arrival and departure manifest data on passengers and crew members; eligibility status of visitors to travel to the United States under the Visa Waiver Program (VWP); I-94 arrival and departure data; and inbound and outbound trade information.
- ***DoS Consular Consolidated Database (CCD):*** Information input into LeadTrac may include biographical information, photographs, and visa revocation/issuance information on visa applicants as well as third party information such as information on applicant family members or employers.
- ***DHS Enforcement Integrated Database (EID):*** Information input into LeadTrac may include information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations conducted by ICE, CBP, and U.S. Citizenship and Immigration Services (USCIS).



Other sources: During the lead work-up process, NSID personnel search a variety of government databases and non-government sources and copy-paste or manually input relevant information into LeadTrac. These sources include but are not limited to ADIS, SEVIS, EID, TECS, CCD, CLAIMS 3, IDENT, FALCON Search & Analysis System, CBP's Analytical Framework for Intelligence, the Office of Biometric Identity Management's Secondary Inspection Tool, and INTERPOL's Criminal Data Access Management System.¹⁰ Similarly, personnel may copy relevant data they find by conducting internet searches and using commercial databases that provide aggregated publicly available information obtained from social media and other internet sites.

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

Yes. NSID personnel use multiple commercial data provider services during the lead work-up process to obtain relevant information on suspected status violators and organizations. The information these services provide is from open (i.e., publicly available) sources and is used to augment the independent research efforts conducted by NSID personnel and advance the investigation of the suspected violator for appropriate enforcement action.

To initiate a search for relevant data NSID personnel upload a limited set of biographical information to the commercial data provider's server in an encrypted, password protected file. The data providers query a wide range of sources, and present the resulting information to NSID personnel who access the commercial provider's results via a secured (HTTPS) and password-

¹⁰ For reference, the PIAs for these systems may be found at the locations below:

- DHS/CBP/PIA-024(a) Arrival and Departure Information System (ADIS): <http://www.dhs.gov/publication/arrival-and-departure-information-system>.
- DHS/ICE/PIA-001(a) Student and Exchange Visitor Information System (SEVIS): http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_sevis.pdf
- DHS/ICE/PIA-015 Enforcement Integrated Database (EID): http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_eid.pdf
- DHS/CBP/PIA-009 TECS System CBP Primary and Secondary Processing (TECS): http://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-tecs-december2010_0.pdf
- DoS Consular Consolidated Database PIA (CCD): https://foia.state.gov/docs/PIA/ConsularConsolidatedDatabase_CCD.pdf
- DHS/USCIS/PIA-016 Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3): http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_cis.pdf
- DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) (includes Secondary Inspection Tool): <http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf>
- DHS/ICE/PIA-032(a) FALCON Search & Analysis System (FALCON-SA): http://www.dhs.gov/sites/default/files/publications/privacy_pia_ice_falconsa_january2014.pdf
- DHS/CBP/PIA-010 Analytical Framework for Intelligence (AFI): http://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_afi_june_2012_0.pdf



protected website. NSID personnel review and analyze results with the express purpose of updating or enhancing the subject's profile in LeadTrac. They cross-reference the new information with the subject's existing profile to ensure the information is relevant to that subject, and assess its timeliness before updating the subject's LeadTrac record. For reference purposes, LeadTrac specifically identifies the source of the information as the commercial data provider within the subject's record. Updated leads are subsequently transmitted to the appropriate field office for further investigation. If no or insufficient information is returned during the initial search, the commercial data providers will continually query public record sources in order to identify and provide updated information. Once leads are deemed non-viable, NSID personnel notify the commercial data providers and, per the terms of the contract, all records associated with those subjects are permanently removed from the providers' information systems.

NSID personnel also collect and analyze information via internet searches to enhance leads. These searches are limited to publicly available information, including social networking and social media sites. NSID personnel copy-paste or summarize relevant information in the appropriate subject records in LeadTrac.

2.4 Discuss how accuracy of the data is ensured.

Training, Standard Operating Procedures, and 100% Review

Extensive system training is provided to NSID personnel who work with LeadTrac, delivered by senior analysts or reviewers. The system training includes guidance on the LeadTrac database and other systems used to conduct research, leveraging established standard operating procedures (SOPs). NSID personnel cross-reference the information from each source against other sources in order to ensure that the information in a record refers to the same subject and to resolve any information that appears to conflict. New analysts are specifically trained on what information belongs in LeadTrac, where that information should be input into the record, and how each system is to be used to find relevant information. Reviewers conduct a secondary review of all records prepared by analysts, and repeat the searches in the source systems to ensure that the data in LeadTrac is accurate and current. This process provides the opportunity to do a final data quality check and update any necessary information. In addition to the above, leads are analyzed to identify areas that are frequently corrected by reviewers. If problem areas are found, either with a particular analyst or overall, the root cause(s) of the problems are identified and rectified through additional training, revisions to SOPs, or by addressing the problem with the system(s) that provide the data.

Corrections to Errors Found in Source Systems and Updating Information

When NSID personnel find a lead that should be split into multiple leads for separate individuals, or find multiple leads or subjects that should be consolidated into a single entity, the system that provided the inaccurate information is notified so that appropriate steps can be taken



to rectify the error. If new or updated information is discovered after a case has been assigned to the field for investigation, NSID personnel will update the record and may also notify the case agent by e-mail or phone with the new information. LeadTrac receives continually updated information from some sources, and sometimes that new information can affect a case that has been assigned to an HSI field office. In addition, HSI's investigation may uncover new information about the subject through additional database checks or other means. HSI agents document their findings in a TECS report with the latest information and, if appropriate, close the case. In turn, the CTCEU receives notification of the case closure and closes the LeadTrac record.

New or updated information pertaining to organizations can be updated by NSID personnel manually in LeadTrac. CTCEU is developing functionality that will enable LeadTrac to continually re-vet information on certain organizations against SEVIS data, and automatically add those updates to the organization's record. This functionality is expected to be available in 2016.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of creating an inaccurate subject record or incorrectly linking the subject records of two separate individuals.

Mitigation: This risk is mitigated by user training which stresses the importance of confirming the accuracy of information entered into LeadTrac and by the use of SOPs that require quality assurance and accuracy checks by designated quality assurance and personnel. LeadTrac has an auditing system built in and periodic reviews of data are conducted to ensure data integrity. NSID personnel are instructed during training that it is better to avoid creating a record or avoid linking two records if there is a question as to the accuracy of the data and/or whether the subjects are one and the same.

Privacy Risk: The use of commercial data may present a risk of data inaccuracy.

Mitigation: This risk is partially mitigated. While any commercial data from multiple sources may contain inaccuracies, ICE promotes data accuracy and integrity when using commercial sources by using credible, industry-wide commercial sources to increase the probability in identifying valid, relevant information. Additionally, all commercial data is considered in combination with United States Government data before a lead is determined viable.

Privacy Risk: Because LeadTrac receives data via both automatic and manual means from multiple systems/sources, there is a risk that LeadTrac may collect more information than is necessary to accomplish the purpose of the program.

Mitigation: This risk is mitigated in two ways: First, LeadTrac does not aggregate data in bulk from systems and sources. It receives data automatically that has already been sorted and enriched and is directly relevant to LeadTrac's lead development purpose. In other words,



LeadTrac automatically receives data where a violation is already suspected. Second, NSID personnel manually collect only data that is relevant for developing a viable lead and that would support the investigative process. Personnel who use this system are trained on both the proper use of the system and on effectively analyzing the information they collect in light of whether it is helpful in developing a lead.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

ICE collects information in LeadTrac about suspected status violators and organizations to help enforce compliance with U.S. immigration laws. Specifically, the information is collected and used to support the following DHS activities: investigating and determining immigration status and criminal history information of individuals; carrying out the appropriate enforcement activity required; determining the likelihood of or confirming a suspected violator's continued presence within the United States and assessing the associated risk level; identifying fraudulent schools and/or organizations and the people affiliated with the school or organization; and providing HSI special agents and ERO with information to further investigate and locate suspected status violators.

The CTCEU also uses LeadTrac information to help allocate its time and resources efficiently and to document and manage compliance enforcement activities. LeadTrac data is also used to assist the CTCEU in establishing, evaluating, and resetting CTCEU's mission and performance objectives based on statistical reports.

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. LeadTrac does not include technology that conducts electronic searches, queries, or analyses to identify a predictive pattern or anomaly.

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

No. Only vetted individuals with a need to access LeadTrac are assigned user accounts that permit them to access the system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of unauthorized access to or disclosure of information contained in LeadTrac. The significance of this risk is enhanced due to LeadTrac's law



enforcement purpose, and the characterization of individuals in the system as suspected status violators.

Mitigation: This risk is mitigated by user training, limiting access to the application, and the practice of operational and information security.

Established SOPs stipulate proscribed and permitted activities, uses, and integrity controls. Additionally, access to LeadTrac is restricted to only those that have the appropriate ICE issued clearance and a “need to know.” Accounts are controlled by the system administrator and are only approved by a CTCEU government manager. In addition, the dissemination of information is controlled and is consistent with DHS’s information sharing policies. Information stored in LeadTrac may be shared with other DHS components, as well as appropriate federal, state, local, tribal, foreign, or international government agencies, when permitted by law. This sharing will only take place after DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in the SORN that covers LeadTrac records.

Additionally, LeadTrac system security features include the use of single sign-on to authenticate users and allow them access to the LeadTrac application. Single sign-on aligns with DHS Personal Identity Verification mandates. Finally, all communications with other government agencies are through secure channels.

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.

ICE and other DHS components provide notice, when necessary, through the publication of PIAs, SORNs, and other notifications deemed appropriate by the DHS component. The DHS/ICE-009 External Investigations SORN provides general notice that lead information about potential immigration law violators is collected, as will the forthcoming LeadTrac SORN. Certain national security, intelligence, and law enforcement collections may not provide advance notice, or may not provide notice through a PIA, because to do so would jeopardize the ability to collect the information.

As discussed in section 2.3, CTCEU subscribes to commercial third-party data provider services, and uses these databases to find information to assist in investigations. The data in these databases is collected by commercial entities from their own sources for the purpose of selling it to other parties, and is not collected on behalf of or at the request of ICE. These data services are responsible for providing the appropriate notice to individuals whose information they collect under applicable laws.



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

Because LeadTrac does not directly collect information from individuals, and because data collected by LeadTrac is for DHS law enforcement purposes, individuals do not have an opportunity to consent to the use of this data.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not be aware their information may be contained within the LeadTrac system, or that it may rely on third-party commercial sources, social networking and social media, and other publicly available internet data.

Mitigation: This risk is partially mitigated. Commercial sources may provide some notice, but that is controlled by the individual providers. ICE mitigates this risk by the public notice provided through this PIA and the SORN. Additionally, individuals will receive notice of the collection of some of the information LeadTrac receives from other sources when they go through application processes (e.g., visa or immigration benefit applications).

Section 5.0 Data Retention by the project

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

Under the NARA-approved records retention schedule for LeadTrac, records must be retained for 75 years. ICE intends to request NARA approval to retain LeadTrac records for 25 years from the date the record was created. Under this schedule, records would be kept as active in LeadTrac for 20 years, and archived for an additional five-year period. After the 25-year period, the information would be destroyed or, if deemed necessary, retained further under a reset retention schedule. The 25-year period provides reasonable assurance that the records of subjects who may be encountered multiple times over a prolonged period of time will be linked.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information contained in LeadTrac will be retained for longer than is needed to accomplish the purpose for which it was originally collected.

Mitigation: This risk is minimal, as the current 75-year retention period for LeadTrac records is consistent with the retention schedules for other investigative records. Because the data in LeadTrac is not unique, ICE is proposing to reduce the retention period for this system to 25 years. This retention period will support the effective enforcement of United States immigration laws by ensuring that leads pertaining to subjects who are encountered repeatedly over a span of time can be linked. Additionally, under the schedule ICE will propose, ICE would be able to archive records at an earlier time when appropriate (e.g., death of subject, subsequent naturalization).



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.

LeadTrac information may be shared with other DHS components, as well as certain federal, state, local, tribal, foreign, or international government agencies for the purposes of safeguarding national security pursuant to applicable laws and within the bounds of official Memoranda of Understanding (MOUs) and Memorandums of Agreement. LeadTrac information is also shared with various federal, state, local, tribal, and foreign agencies on a case-by-case basis when a need to know has been confirmed and ICE has authority to do so under applicable law.

The exact method of disclosure during investigations can vary, but all CTCEU disclosures are made in accordance with DHS policies on the safeguarding of Sensitive PII. Information is generally transmitted electronically or orally via phone call to external organizations on a case-by-case basis. Information transmitted electronically to certain external organizations is done via e-mail, utilizing password protection and encryption. Information can also be transmitted manually by way of hand delivery or secure courier service.

ICE also shares limited identifying information of suspected status violator data with contracted commercial data providers on a routine basis so that they may conduct batch and ad hoc searches of their proprietary systems to enhance information pertaining to potential leads. NSID personnel upload a limited set of biographical information to the commercial data provider's server in an encrypted, password-protected file. The data providers query a wide range of sources, and present the resulting information to NSID personnel who access the commercial provider's results via a secured (HTTPS) and password-protected website.

Finally, ICE produces LeadTrac statistical reports and data that may be provided to Congress, auditors, and other external recipients; however, these reports do not contain PII.

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

The sharing described above is compatible with the original purpose for collection, namely to generate leads for field investigation to assist with the enforcement of U.S. immigration laws. All external sharing falls within the scope of applicable law, including the published routine uses in the applicable SORN.

6.3 Does the project place limitations on re-dissemination?

Federal agencies that receive LeadTrac information are subject to the Privacy Act and, as such, may not re-disclose information without clear authority to do so. Non-government



organizations (i.e., commercial data providers) with which ICE shares LeadTrac information are prohibited under terms of their contracts from re-disseminating LeadTrac information. They are also required to maintain reasonable physical, technical, and administrative safeguards to appropriately protect the shared information, and notify CTCEU if they become aware of any breach of security of interconnected systems or potential or confirmed unauthorized use or disclosure of personal information.

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

LeadTrac administrators or their specified designees log and maintain copies of all recurring weekly reports and ad hoc requests that are sent to external agencies on a secure shared drive with restricted access.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information may be shared with outside Government and non-government entities without a need to know.

Mitigation: In order to reduce the risk of inappropriate dissemination of information, LeadTrac has implemented IT security processes that include audit logs and single sign-on capability. Additionally, ICE employees and contractors are trained on the appropriate sharing of the PII, and to contact the ICE Privacy Office if they are not certain whether information sharing is appropriate. Data owners ensure that privacy risks are mitigated through data sharing agreements that detail prohibitions on re-disclosure and require physical, technical, and administrative controls. Commercial data providers are restricted from re-disclosing LeadTrac information pursuant to the terms of their contracts with ICE. As an added precautionary measure, CTCEU is developing functionality in LeadTrac that will automatically mark paper records generated from the system with a “Law Enforcement Sensitive” header and footer. This functionality is expected in 2016.

Section 7.0 Redress

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

Individuals seeking notification of and access to any record contained in this system of records may submit a request in writing to the ICE Freedom of Information Act (FOIA) officer by mail or facsimile:

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street SW, Stop 5009



Washington, D.C. 20536-5009

(202) 732-0660

<http://www.ice.gov/foia/>

All or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing individual access to records contained in LeadTrac could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to records could also permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, or avoid detection or apprehension.

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

Individuals seeking to correct records contained in this system of records, or seeking to contest its content, may submit a request in writing to the ICE Privacy and Records Office by mail:

U.S. Immigration and Customs Enforcement

Privacy and Records Office

Attn: Privacy Branch

500 12th Street SW, Stop 5004

Washington, D.C. 20536-5004

(202) 732-3300

<http://www.ice.gov/management-administration/privacy>

All or some of the requested information may be exempt from correction pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing individual access to records contained in LeadTrac could inform the subject of an actual or potential criminal, civil, or regulatory investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, or avoid detection or apprehension.

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

The procedure for submitting a request to correct information is outlined in this PIA and the associated SORN. As stated above, individuals may submit requests for information and correction as permitted by the Privacy Act, which will be reviewed and corrected on a case-by-case basis.



7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals or organizations will be unable to meaningfully control the use of their data as maintained in this system, or determine whether the system maintains records about them.

Mitigation: Because the records in LeadTrac are aggregated from various other databases within DHS components and offices as well as other federal, state, local, tribal, and international agencies and commercial databases, individuals' and organizations' rights to be notified of the existence of data about them, and to direct how that data may be used by ICE, are limited. Permitting individuals or organizations to direct the agency's use of their information would interfere with the intended law enforcement use of the system. Individuals or organizations may also have the option to seek access to and correction of their data directly from the agencies or organizations that originally collected it. Information that is corrected in the original data source can only be updated in LeadTrac when the information is again accessed in the source database or based upon a request of an individual or organization, or when ICE becomes aware of inaccuracies of the information.

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?

This PIA is subject to periodic revision in the case that (a) additional data sources not described elsewhere in the document begin to be used in the routine processing of LeadTrac records; (b) analytical data tools that identify predictive patterns or anomalies are introduced, or (c) if any change to the mission supported by LeadTrac leads to changes in the way data is collected, analyzed, or disseminated to law enforcement partners. Any proposed change to the scope of LeadTrac that would go beyond the bounds of what is described in this PIA would result in an updated PIA.

With regard to regular use within the bounds of this PIA, LeadTrac relies on built-in auditing capabilities. LeadTrac contains an auditing mechanism to track general user activity (application logon/logoff) as well as user activity within each record. LeadTrac automatically records the user ID and date/time stamp whenever a record is accessed or modified by a user. This includes the date and time each user logs onto the system, the records that are created, viewed or edited, the actual changes to the data, the time at which the record was changed, and the user that changed the data. In addition, all search requests will be logged. This audit trail persists in the database. In this way, designated personnel at the CTCEU are able to track user activities and ensure accountability.



Individuals who are found to access or use the LeadTrac data in an unauthorized manner will be disciplined in accordance with ICE policy. These and other controls described in this PIA ensure the system is used only by authorized users for the intended purpose. Suspected violations of law or user rules of behavior are reported to the Office of the Information System Security Manager team in accordance with the DHS security standards, as well as the ICE Office of Professional Responsibility.

LeadTrac also relies upon the security of the ICE Network to ensure that information is used only in support of the practices described in this PIA. Only users who have access to the ICE Network and are granted access to LeadTrac are able to log onto the LeadTrac application using their IRMNET credentials. All users must have first read and signed the DHS Rules of Behavior for DHS IT systems to obtain access. Only the LeadTrac administrator and developers have access to the database and server through an administrative account. The technical staff have user IDs by name and ID numbers and role(s) are attached to that name. Access to the CTCEU facility is subject to a variety of physical security controls.

ICE has implemented various other security controls and safeguards that help to ensure only authorized users are able to access the information in the system. These controls include single sign-on and periodic reviews of user lists by CTCEU managers to ensure only current CTCEU employees and contractors hold user accounts. As soon as an ICE employee or contractor is transferred out of the CTCEU, his or her LeadTrac account is archived and access to the LeadTrac application will be revoked.

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

All personnel who have access to the ICE network are also required to take annual privacy and security training, which emphasizes the DHS Rules of Behavior and other legal and policy restrictions on user behavior. Additionally, system users receive training on appropriate uses of LeadTrac as part of CTCEU's Operations Training.

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

Only ICE personnel who require access to the functionality and data in LeadTrac as a part of the performance of their official duties will be granted access. CTCEU management oversees and approves the assignment of user accounts to ICE personnel, and at present only CTCEU staff and HSI personnel are authorized to access the system.

Only ICE network authenticated users will be granted access to LeadTrac. Authorized users access LeadTrac over the ICE network from ICE standard workstations. The LeadTrac



administrator establishes user accounts and updates user identification, role, and access profiles as changes are needed. Access roles are assigned by a supervisor based on the user's job responsibilities, and implemented by a LeadTrac administrator. Access roles are reviewed regularly to ensure that users have the appropriate access. Individuals who no longer require access are removed from the access list.

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 sharing agreements and MOUs are reviewed by the program manager, component Privacy Officer, and counsel, and then sent to DHS for formal review.

Responsible Officials

Amber Smith
Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

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

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security



APPENDICES

Appendix A – LeadTrac Modernization System Template

Lead Source:

List the name of lead source/ cross-agency effort.

Purpose and Use:

Provide a detailed description for why the data is being provided to run through LeadTrac (e.g., why DoD provided ICE with an Excel spreadsheet of data to run through LeadTrac).

Authority:

Provide the legal authorities for ICE to receive the information to run through LeadTrac for this lead source/project. Also, provide the legal authorities for the appropriate use for the information provided.

Individuals Impacted:

Provide a list of individuals (i.e., members of the public) whose information will be contained in the system.

Data Elements Collected:

Provide a specific description of information that may be collected, maintained, and/or generated by the project lead. Highlight any collection and maintenance of PII and Sensitive PII.

Sources of Information:

List systems, etc. that provide information in support of this effort.

Information Sharing:

Define the content, scope, and authority for information sharing internal and external to DHS.

Notice:

Provide a specific description of how or whether the impacted individuals are notified of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

SORN Coverage:

List the SORN(s) under which this data collection and maintenance is covered.

Records Retention Period:

List any relevant records retention schedules set by the National Archives and Records Administration (NARA) under which this data collection is covered.



Appendix B

Lead Source:

Department of Defense (DoD)

Purpose and Use:

CTCEU works closely with the DoD to assess members of foreign militaries applying for positions at U.S. military academies, verify immigration status for nonimmigrant participants in DOD-sponsored expedited naturalization programs, and to locate foreign military members whom have gone Absent Without Leave (AWOL) from DOD-sponsored training in the United States. DoD will send CTCEU the applicant's information, and CTCEU will check the applicant's background using numerous government databases and open source and analysis resources to provide vetting results back to DoD. DoD is responsible for determining the eligibility of the applicant.

If a nonimmigrant foreign military member does not comply with DoD requirements (i.e., going AWOL) or if a nonimmigrant service member were to lose or withdraw from DoD-sponsored immigration status, DoD notifies CTCEU. CTCEU then works with DoD to investigate and locate those individuals. Any leads generated from CTCEU are then sent to HSI field offices and DoD partners for further action.

Authority:

ICE has been authorized to collect information in LeadTrac by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law 104-208; the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106-215; the Visa Waiver Permanent Program Act of 2000 (VWPPA), Public Law 106-396; The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (U.S.A. PATRIOT Act) of 2001, Public Law 107-56; the Enhanced Border Security and Visa Entry Reform Act (Border Security Act), Public Law 107-173; and the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53.

DoD Authorities:

- 10 USC § 4345(a) allows for the Secretary of the Army to prescribe any regulations or requirements regarding the U.S. Service Academies participation in a foreign exchange program.
- Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security on Information Sharing and Technology Partnering Relating to Identity Verification and Screening Activities (March 3, 2011);



- Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (March 4, 2003), as amended;

Individuals Impacted:

International military students, nonimmigrant participants in DoD programs for expedited naturalization, and known relatives and non-family associates of subjects of investigation.

Data Elements Collected:

- Full name and aliases;
- Country of citizenship/origin;
- Passport and visa information;
- Effective date and time of absence;
- Date of Birth;
- Place of Birth;
- Last Known Location;
- Listed addresses (i.e. current, home of record);
- Phone Number(s);
- Case Identification/Work Control Number;
- Training status;
- Travel circumstances;
- Names and contact information of known relatives in the United States;
- Information on U.S. driver's license;
- Branch of service and military occupation specialty;
- Military Identification numbers and copies of any DoD identification cards issued;
- Immigration status and history;
- Criminal history;
- Investigative results; and
- Any location information or derogatory information derived from open source systems.



Sources of Information:

CTCEU receives information from DoD manually on a case-by-case basis.

Information Sharing:

CTCEU provides an “AWOL Notification Letter” to Department of State (DoS) and requests a “No Status Letter” from DoS that will revoke the individual’s visa. CTCEU then issues a collateral investigative request, also known as a lead, to the appropriate field office, notifies the Attaché at the appropriate Embassy. CTCEU also keeps DoD informed of the case status and results of its investigations.

Notice:

LeadTrac does not collect information directly from individuals. ICE and other DHS components provide notice, when necessary, through the publication of PIAs, SORNs, and other notifications deemed appropriate by the DHS component. In addition, both the DHS/ICE-009 External Investigations SORN and DHS/ICE-015 LeadTrac SORN provide general notice that lead information about potential immigration law violators is collected.

Notice to individuals is limited in this case because giving notice to an individual could undermine ICE’s efforts to locate the individual and take the appropriate enforcement actions. It is also limited because the collection of information generally occurs when the suspected status violator’s location is unknown.

SORN Coverage:

Information in LeadTrac is covered by DHS/ICE-015 LeadTrac SORN. CTCEU’s activities as an investigative unit is also covered by DHS/ICE-009 External Investigations SORN. All sharing with DoD programs is covered under Routine Uses I and K of the LeadTrac SORN, which allow the disclosure of information to other agencies for the purposes of gathering intelligence and coordinating or deconflicting investigations. Sharing with DoS is in accordance with Routine Use R of the External Investigations SORN, which covers disclosures to DoS regarding an enforcement action that may have transnational implications.

Records Retention Period:

Under the NARA-approved records retention schedule for the identification, investigation, apprehension, removal of aliens unlawfully entering or present in the United States and to facilitate entry of individuals into the United States (DAA-0563-2013-0001-0006), records must be retained for 75 years. Under the External Investigations SORN, records related to investigations are retained for twenty (20) years after a case closes in accordance with legacy customs records schedules (N1-36-86-1-161.3 (inv 7B)). ICE is in the process of drafting an agency-wide records schedule that will require ICE to hold investigative records for 25 years.



Appendix C

Lead Source:

Department of State (DoS)

Purpose and Use:

CTCEU works in coordination with DoS to ensure that all nonimmigrant aliens in the United States who have had their visas revoked on national security or counterproliferation grounds are investigated, located, and—if possible—removed from the United States.

If a nonimmigrant visa holder violates the terms of his or her visa or is a national security or proliferation concern, CTCEU thoroughly investigates the matter and generates leads for further action by HSI field offices. When DoS revokes a visa because of national security concerns, they notify CTCEU. CTCEU pulls all national security visa revocations from the CCD. CTCEU fully reviews the lead and, if the subject of the revocation is found to be present in the United States, a collateral investigative request is forwarded to the appropriate HSI field office for further investigation to determine the location of the subject, if the subject is in violation of the terms of their admission, and if the subject can be placed in removal proceedings.

Authority:

ICE has been authorized to collect information in LeadTrac by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law 104-208; the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106-215; the Visa Waiver Permanent Program Act of 2000 (VWPPA), Public Law 106-396; The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (U.S.A. PATRIOT Act) of 2001, Public Law 107-56; the Enhanced Border Security and Visa Entry Reform Act (Border Security Act), Public Law 107-173; and the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53.

DoS Authorities:

The exception to the confidentiality provisions of Section 222(f) of the Immigration and Nationality Act for the use of visa records for the administration or enforcement of U.S. laws.

Individuals Impacted:

All nonimmigrants whose visas have been revoked on national security or counterproliferation grounds and their family and known associates.

Data Elements Collected:

- Full name and aliases;



- Gender;
- Address information;
- Contact information (phone numbers and email addresses);
- Date of Birth;
- Place of Birth;
- Country of Citizenship;
- Travel information;
- Passport and visa information, including validity information, number of entries, and information submitted as part of visa applications;
- Information from DoS regarding Security Advisory Opinions (SAO), recommended actions, visa annotations, and case and refusal comments;
- Photographs;
- Federal Identification Numbers, including Social Security number (SSN), Fingerprint Identification Number (FIN), Admission Number, and other identifying numbers (i.e., driver's license);
- Student and Exchange Visitor Information System information¹¹ (SEVIS ID, student ID, SEVIS record status, program start/end dates);
- Educational status and activity (i.e., affiliated foreign schools, current schools, courses of study);
- Information about associates, including points of contact, family, and sponsors (names, dates of birth, address and contact information);
- Applications and petitions filed with USCIS;
- Information related to participation in educational or exchange programs, including information about the individuals (possibly including U.S. citizens) who operate those programs;
- Geolocation of addresses provided by other systems;
- Information about criminal history or prior encounters with immigration enforcement;
- Information about vehicles related to the individual; and

¹¹ See DHS/ICE/PIA-001 Student and Exchange Visitor Program (SEVP), available at www.dhs.gov/privacy.



- Any location and derogatory information derived from open source systems.

Source(s) of Information:

DoS Consular Consolidated Database (CCD)

Information Sharing:

CTCEU fully reviews leads from CCD and when the subjects of revocations are found to be present in the United States or a visa holder is determined to violate the terms of their admission, a collateral investigative request is forwarded to the appropriate HSI field office for further investigation. The investigation at the field level is coordinated and deconflicted with law enforcement partners.

Notice:

LeadTrac does not collect information directly from individuals. ICE and other DHS components provide notice, when necessary, through the publication of PIAs, SORNs, and other notifications deemed appropriate by the DHS component. In addition, the both the DHS/ICE-009 External Investigations SORN and DHS/ICE-015 LeadTrac SORN provide general notice that lead information about potential immigration law violators is collected.

Notice to individuals is limited in this case because doing so could undermine ICE's efforts to locate the individual and take the appropriate enforcement actions. It is also limited because the collection of information generally occurs when the suspected status violator's location is unknown.

SORN Coverage:

Information in LeadTrac is covered by the DHS/ICE-015 LeadTrac SORN. Other information gathered during CTCEU's investigative efforts is covered by DHS/ICE-009 External Investigations SORN. Sharing with DoS is covered by Routine Use T in a forthcoming update to the External Investigations SORN, which explicitly states that ICE can share PII with the DoS for purposes of informing DoS's visa issuance, revocation, and renewal decisions.

Records Retention Period:

Under the NARA-approved records retention schedule for the identification, investigation, apprehension, removal of aliens unlawfully entering or present in the United States and to facilitate entry of individuals into the United States (DAA-0563-2013-0001-0006), records must be retained for 75 years. Under the External Investigations SORN, records related to investigations are retained for twenty (20) years after a case closes in accordance with legacy customs records schedules (N1-36-86-1-161.3 (inv 7B)). ICE is in the process of drafting an agency-wide records schedule that will require ICE to hold investigative records for 25 years.



Appendix D

Lead Source:

Transportation Security Administration (TSA)

Purpose and Use:

CTCEU works collaboratively with TSA's Law Enforcement Investigative Unit (LEIU) in identifying individuals who have obtained, are applying for, or are renewing a Transportation Worker Identity Credential (TWIC) or a Hazmat Material Endorsement (HME), which is used to obtain a Commercial Driver's License (CDL). These documents can be used to gain access to critical infrastructure areas or sites. CTCEU investigates applicants who are suspected of misrepresenting themselves by fraudulently claiming lawful permanent resident (LPR) or U.S. citizen (USC) status in order to obtain a TWIC or HME. If CTCEU determines that a nonimmigrant is in violation of his or her status of fraudulently claiming LPR/USC status a lead is forwarded to the appropriate HSI field office for further investigation.

Separately, the Alien Flight Student Program (AFSP) is a TSA initiative enacted to screen prospective flight student candidates who are not U.S. citizens before they are allowed to undergo pilot training. This program was created in response to the September 11, 2001, terrorist attacks, in recognition of the fact that the individuals who piloted the hijacked aircrafts learned to fly at U.S. flight schools. The mission of the AFSP is to ensure that foreign students seeking training at flight schools regulated by the Federal Aviation Administration (FAA) do not pose a threat to aviation or national security. Potential foreign flight students apply to TSA AFSP and are vetted by a TSA investigator. If no derogatory information is found during TSA's vetting the applicant is approved by the AFSP and is permitted to attend flight school. However, if derogatory information is discovered during TSA's investigation, TSA sends the applicant's information to CTCEU. CTCEU investigates the subject of a referral through open source and government database queries. If CTCEU determines an AFSP applicant is in violation of his/her status or not authorize to take flight training, a lead is forwarded to the appropriate HSI field officer for further investigation. CTCEU then returns the information back to TSA for final determination on the applicant.

TSA's database to track alien flight students (maintained as part of TSA's Alien Flight Student Program (AFSP)¹²) is the source used by CTCEU to gather information for the program.

Authority:

ICE has been authorized to collect information in LeadTrac by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law 104-208; the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106-

¹² See DHS/TSA/PIA-026 Alien Flight Student Program (AFSP), available at www.dhs.gov/privacy.



215; the Visa Waiver Permanent Program Act of 2000 (VWPPA), Public Law 106–396; The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (U.S.A. PATRIOT Act) of 2001, Public Law 107–56; the Enhanced Border Security and Visa Entry Reform Act (Border Security Act), Public Law 107–173; the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53; the Aviation and Transportation Security Act of 2001.

Individuals Impacted:

Visa overstays who have received flight training in the United States, students not authorized to take flight training in the United States, and individuals that have applied for TWIC or HME credentials.

Data Elements Collected:

- Full name and aliases;
- Gender;
- Date of Birth;
- Place of Birth: City, State, Country;
- Country of Citizenship;
- Identifying numbers such as Alien Registration Number, Social Security number, Fingerprint Identification Number (FIN);
- Information about the individual’s visa (including information from the application) and passport;
- Address and contact information;
- Travel information;
- Immigration history;
- SEVIS information (SEVIS ID, school name/code, status, course of study, program start and end dates);
- Information about the individual’s attendance at a flight school, including information about the school and individuals associated with that flight training program;
- Associate information (name, date of birth, relationship, etc.); and
- Any location and derogatory information found in open source systems.



Sources of Information:

TSA's Alien Flight Student Program Database,¹³

Information Sharing:

CTCEU shares investigative information manually with TSA throughout the investigative process. If CTCEU determines there is evidence of fraud or a violation of a nonimmigrant's terms of admission, a lead is forwarded to the appropriate HSI field office for further investigation.

Notice:

LeadTrac does not collect information directly from individuals. ICE and other DHS components provide notice, when necessary, through the publication of PIAs, SORNs, and other notifications deemed appropriate by the DHS component. In addition, the both the DHS/ICE-009 External Investigations SORN and DHS/ICE-015 LeadTrac SORN provide general notice that lead information about potential immigration law violators is collected.

Notice to individuals is limited in this case because doing so could undermine ICE's efforts to locate the individual and take the appropriate enforcement actions. It is also limited because the collection of information generally occurs when the suspected status violator's location is unknown.

A Privacy Act statement is published at the bottom of an individual's application for TWIC or HME certification. Individuals are notified in the statement that the information may be shared for investigation and adjudication of the application.

SORN Coverage:

Information in LeadTrac is covered by DHS/ICE-015 LeadTrac SORN. CTCEU investigative activity is also covered by the DHS/ICE-009 External Investigations SORN.

Records Retention Period:

Under the NARA-approved records retention schedule for the identification, investigation, apprehension, removal of aliens unlawfully entering or present in the United States and to facilitate entry of individuals into the United States (DAA-0563-2013-0001-0006) records must be retained for 75 years. Under the External Investigations SORN, records related to investigations are retained for twenty (20) years after a case closes in accordance with legacy customs records schedules (N1-36-86-1-161.3 (inv 7B)). ICE is in the process of drafting an agency-wide records schedule that will require ICE to hold investigative records for 25 years.

¹³ See DHS/TSA/PIA-026 Alien Flight Student Program (AFSP) available at www.dhs.gov/privacy.



Appendix E

Lead Source:

Federal Bureau of Investigation National Crime Information Center (NCIC)¹⁴

Purpose and Use:

NCIC is a central repository of national criminal records that can be accessed by law enforcement agencies nation-wide. The NCIC operates as a computerized index of criminal justice information that is reported to the FBI by law enforcement agencies throughout the United States and internationally. It contains information on warrants, protection orders, stolen property, wanted persons, missing persons, victims of identity theft, violent gangs, terrorists, and other persons of interest to law enforcement. The NCIC also maintains the Interstate Identification Index (III), which contains automated criminal history record information maintained by state and local law enforcement agencies.¹⁵

NCIC hits (positive identification matches to records in NCIC) on visa overstays are imported into LeadTrac by CBP's Automated Targeting System (ATS)¹⁶ through a daily import. CTCEU uses NCIC to identify overstays who have open wants and warrants or a criminal history. Overstays with wants and warrants are prioritized within CTCEU in its workflow. CTCEU agents and analysts will also check NCIC periodically for updates to a subject's criminal history.

Finally, as part of the Designated School Official (DSO) Suitability Initiative, CTCEU runs NCIC checks on a manual basis. CTCEU receives names and dates of birth (DOBs) of DSOs from the Student and Exchange Visitor Program (SEVP) School Certification Unit (SCU) on a weekly basis and conducts criminal history and background checks using NCIC. SEVP SCU provides the information to CTCEU on all proposed DSOs at the time of application for initial SEVP certification, or whenever a school requests to add a new DSO. The project is working towards reviewing all DSOs as part of the recertification process.

Findings from CTCEU's NCIC checks are forwarded to the SEVP Analysis and Operations Center (SAOC) for determination on whether or not any criminal charges/convictions found by CTCEU meet the threshold established by SEVP for removal of a DSO.

Authority:

Authority to collect information regarding officials and schools certifying to become part of SEVP is covered by 8 § CFR 214.3. CTCEU's use of NCIC to help administrate the INA is authorized by 8 USC 1105.

¹⁴ See Federal Bureau of Investigation Privacy Impact Assessment of the National Crime Information Center available at <https://www.fbi.gov/file-repository/pia-ncic.pdf/view>.

¹⁵ For more information on the Interstate Identity Index see <https://www.bjs.gov/content/pub/pdf/iiince.pdf>.

¹⁶ See DHS/CBP/PIA-006 Automated Targeting System (ATS) available at www.dhs.gov/privacy.



Individuals Impacted:

Individuals who are suspected of overstaying their visa. Individuals who are currently, or apply to become, a Designated School Official.

Data Elements Collected:

- Full name;
- Date of birth;
- Employment information;
- Criminal history; and
- Any tips or investigative leads from outside sources.

Sources of Information:

NCIC

Information Sharing:

CTCEU analysts will derive information from SEVIS and enter it into NCIC for a criminal history check. Any derogatory information will be referred to SEVP and the local HSI field office for further investigation.

Notice:

Visa applicants are informed that their information may be used for criminal background checks at the time of application. DSOs are also given notice that ICE is collecting their information at the time of collection. The form I-17¹⁷ states that designation as a DSO is subject to SEVP approval. LeadTrac does not collect information directly from individuals. ICE provides notice through the publication of this appendix and the ICE Student and Exchange Visitor Information System (SEVIS) PIA.¹⁸ In addition, the DHS/ICE-001 SEVIS SORN notifies the public that ICE collects information from school officials for certifying compliance with Federal regulations. The SORN further notes that the information could be used for law enforcement purposes. In addition, the DHS/ICE-015 LeadTrac SORN provides notice that lead information about potential immigration law violators is collected.

SORN Coverage:

Information in LeadTrac is covered by the DHS/ICE-015 LeadTrac SORN. Any information transferred to SEVP is covered by the DHS/ICE-001 SEVIS SORN. Information

¹⁷ See DHS/ICE/PIA-001 Student and Exchange Visitor Program (SEVP) available at www.dhs.gov/privacy.

¹⁸ See DHS/ICE/PIA-001 Student and Exchange Visitor Program (SEVP) available at www.dhs.gov/privacy.



shared with NCIC is covered under routine use I of the LeadTrac SORN, which allows disclosure to other law enforcement agencies for the collaboration of law enforcement matters.

Records Retention Period:

Under the NARA-approved records retention schedule for the identification, investigation, apprehension, removal of aliens unlawfully entering or present in the United States and to facilitate entry of individuals into the United States (DAA-0563-2013-0001-0006) records must be maintained for 75 years. ICE is in the process of drafting an agency-wide records schedule that will require ICE to hold investigative records for 25 years.



Appendix F

Lead Source:

International Criminal Police Organization (INTERPOL) Program

Purpose and Use:

CTCEU's INTERPOL program was implemented in 2004 as an enforcement collaboration between CTCEU, the Department of Homeland Security (DHS) Office of Biometric Identity Management (OBIM), and INTERPOL. CTCEU reviews National Crime Information Center hits notifying of INTERPOL diffusions (a type of alert)¹⁹ and reviews the corresponding information in NCIC. CTCEU requests verification from INTERPOL on whether the hit is still active and refers actionable leads to HSI field offices for further investigation in cases where the fugitive is believed to be present in the United States and has a potential immigration violation. The goal of this effort is to identify, track, apprehend, and if necessary, remove INTERPOL fugitives in the United States who are in violation of U.S. immigration law. When the subjects of INTERPOL notices are found to be present in the United States, analysts generate a lead in LeadTrac and a collateral investigative request is forwarded to the appropriate HSI field office for further investigation.

Authority:

22 USC § 263A, 8 USC § 1357 & Section 287 of the INA, 19 USC § 1595a, Memorandum of Understanding between the U.S. Department of Homeland Security and the U.S. Department of Justice pertaining to U.S. membership in the International Criminal Police Organization (INTERPOL), management of the INTERPOL-U.S. National Central Bureau, and Related Matters.

Individuals Impacted:

Individuals who have entered the United States and are subjects of investigation by INTERPOL.

Data Elements Collected:

- Full name and aliases;
- Date of birth;
- Country of birth;
- Country of citizenship;
- Physical description (i.e., height, weight, eye color, hair color);

¹⁹ A Diffusion is an informal request for cooperation between member countries of INTERPOL. For more information see <https://www.interpol.int/en/How-we-work/Notices/About-Notices>.



- Photographic images;
- INTERPOL Notice Type (Black; Blue; Green; No Color; Orange; Purple; Red; Yellow);²⁰
- Issuing Country;
- INTERPOL Case number;
- Criminal history;
- Immigration history;
- Any location or derogatory information derived from open source systems;
- Associate name;
- Associate relationship; and
- Associate address.

Sources of Information:

INTERPOL's Criminal Data Access Management System²¹.

Information Sharing:

CTCEU fully reviews leads from INTERPOL and, when the subjects of INTERPOL notices are found to be present in the United States, a collateral investigative request is forwarded to the appropriate HSI field office for further investigation. The investigation at the field level is coordinated and deconflicted with law enforcement partners

Notice:

LeadTrac does not collect information directly from individuals. ICE provides notice through the publication of this PIA appendix. In addition, the DHS/ICE-015 LeadTrac SORN provide general notice that lead information about potential immigration law violators is collected.

Notice to individuals is limited in this case because doing so could undermine ICE's efforts to locate the individual and take the appropriate enforcement actions. It is also limited because the collection of information generally occurs when the suspected status violator's location is unknown.

Most INTERPOL notices are restricted to law enforcement use only, but INTERPOL

²⁰ See www.interpol.int/en/How-we-work/Notices/About-Notices.

²¹ For more information on INTERPOL privacy policies see www.interpol.int/content/download/5694/file/INTERPOL%20Rules%20on%20the%20Processing%20of%20Data-EN.pdf.



does post some public notices of wanted individuals.²²

SORN Coverage:

Information in LeadTrac is covered by the DHS/ICE-015 LeadTrac SORN. All sharing with INTERPOL is covered under Routines Use I, J, and K, which allow the disclosure of information to law enforcement agencies for the purposes of gathering intelligence and coordinating or deconflicting investigations.

Records Retention Period:

Under the NARA-approved records retention schedule for the identification, investigation, apprehension, removal of aliens unlawfully entering or present in the United States and to facilitate entry of individuals into the United States (DAA-0563-2013-0001-0006) records must be retained for 75 years. ICE is in the process of drafting an agency-wide records schedule that will require ICE to hold investigative records for 25 years.

²² See www.interpol.int/en/how-we-work/notices/view-red-notices.



Appendix G

Lead Source:

Open Source Systems

Purpose and Use:

CTCEU extracts pertinent information from open source systems and social media regarding CTCEU investigative subjects including criminals, fugitives, nonimmigrant violators, and individuals of national security concerns. This is accomplished by focusing their open source analyses on media, blogs, public hearings, conferences, academic websites, and social media websites such as Twitter, Facebook, and LinkedIn. Open Source analysts also review and assess other publicly available information, including radio, television, print media geospatial sources, internet sites, and specialized publications.

CTCEU uses government databases to close leads (resolve a lead or determine it to be non-viable) prior to searching open source systems. The information extracted through open source analysis helps identify location of subjects, violation of terms of admission for visa holders, and other actionable intelligence. CTCEU also uses a third-party open source vetting platform. This platform periodically searches publicly available information on the internet for updates regarding subjects of investigations.²³ The analyst then completes a review of the platform results and conducts manual open source analysis to establish actionable intelligence. This assists analysts in identifying derogatory and location information related to subjects of investigation. Analysts will record analysis summaries in LeadTrac and a separate access database. LeadTrac will hold and track all leads.

Authority:

Executive Order 12333; Security Act of 2002, as amended, Pub. L. No. 107-296, 116 Stat. 2135 (2002); Immigration and Nationality Act of 1952, as amended, U.S. Code Title 8; DHS Delegation No. 7030.2, Delegation of Authority to the Assistant Secretary of U.S Immigration and Customs Enforcement; ICE Delegation No. 0001, Delegation of Authority to the Directors, Detention and Removal and Investigations, and to Field Office Directors, Special Agents in Charge and Certain Other Officers of the Bureau of Immigration and Customs Enforcement; 8 CFR § 2.1, Authority of the Secretary of Homeland Security.

²³ The platform also provides a query feature to compare one facial image the platform returned to other images already returned from a search. In those instances, CTCEU analysts may select an image that was returned by conventional query method (e.g., name search) and the vendor will use the comparison function to search for similar images within that same search return.



Individuals Impacted:

Individuals determined to be criminals, fugitives, nonimmigrant violators, and targeted national security concerns, as well as individuals issued visas from designated consular posts.

Data Elements Collected:

- Full name and aliases;
- Date of Birth;
- Address;
- Any identifying numbers found in government systems;
- E-mail address;
- Employment information;
- Social media accounts/web identities/usernames;
- Screenshots of posts and relevant comments made by a subject or associate;
- Derogatory information viewed on social media posts;
- Location information located on social media posts (including geotags and locations observed in posts), last account activity date, URLs of relevant posts;
- Associate name;
- Associate relationship;
- Associate addresses; and
- Social media posts from others that contain the subject of the investigation.

Information Sharing:

CTCEU uses open source systems to support its efforts and may therefore share open source information with any entity described within the PIA. This includes the FBI through joint task forces, DoD, INTERPOL, SEVIS, TSA, and DoS. Open source information may be forwarded to the appropriate HSI field office for further investigation. The investigation at the field level may also be coordinated and deconflicted with law enforcement partners.

Sources of Information:

Open Source Systems

Notice:

LeadTrac does not collect information directly from individuals. ICE provides notice of information entering its system through the publication of this appendix. In addition,



DHS/ICE-015 LeadTrac SORN provides notice that lead information about potential immigration law violators is collected.

SORN Coverage:

Information in LeadTrac is covered by the DHS/ICE-015 LeadTrac SORN. Investigative activities conducted by CTCEU are also covered by DHS/ICE-009 External Investigations SORN. All information is shared in accordance with Routine Use I of the LeadTrac SORN which allows the disclosure of information to other agencies for coordinating or deconflicting investigations.

Records Retention Period:

Under the NARA-approved records retention schedule for the identification, investigation, apprehension, removal of aliens unlawfully entering or present in the United States and to facilitate entry of individuals into the United States (DAA-0563-2013-0001-0006), records must be retained for 75 years. Under the External Investigations SORN, records related to investigations are retained for twenty (20) years after a case closes in accordance with legacy customs records schedules (N1-36-86-1-161.3 (inv 7B)). ICE is in the process of drafting an agency-wide records schedule that will require ICE to hold investigative records for 25 years.