Privacy Impact Assessment
for the

One DHS Overstay Vetting Pilot

DHS/ALL/PIA-041

December 29, 2011

Contact Point
Screening Coordination Office
DHS Policy

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

DHS is conducting the One DHS Overstay Vetting Pilot to improve DHS' ability to identify and vet foreign nationals who have remained in the United States beyond their authorized period of admission (overstays). The pilot will attempt to streamline data sharing between the National Protection and Programs Directorate's United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program, U.S. Customs and Border Protection (CBP), and U.S. Immigration and Customs Enforcement (ICE). The overstay vetting process is covered by existing PIAs for the CBP Automated Targeting System (ATS),[1] US-VISIT Technical Reconciliation Analysis Classification System (TRACS),[2] and US-VISIT Arrival Departure Information System (ADIS).[3] In addition to this existing coverage, US-VISIT has worked with the DHS Privacy Office to complete this PIA specific to the Overstay Vetting Pilot to add another layer of analysis and transparency to this specific process which can be updated as the program matures. Data sharing conducted through this program allows DHS to better identify which individuals have overstayed their authorized periods of admission, and of those overstays, which are the highest law enforcement or national security priority for enforcement action by ICE. DHS is conducting this PIA because the pilot increases the sharing within DHS of personally identifiable information (PII) about travelers.

Overview

DHS is administering the One DHS Overstay Vetting Pilot for two purposes: 1) to reduce misidentification of overstays (hereafter referred to as misidentified overstays); and 2) to identify which vetted overstays are of greater priority for enforcement actions by ICE. To reduce misidentified overstays, US-VISIT is matching additional CBP, United States Citizenship Immigration Services (USCIS), and ICE biographic data against potential overstay leads that may indicate the lead has left the country or changed immigration status and thus is not an in-country overstay.[4] To identify potential enforcement priorities, US-VISIT is reviewing lead data from existing CBP law enforcement and national security lists and scenario-based traveler

[1] See ATS PIA, DHS/CBP/PIA-006, and ATS SORN, DHS/CBP-006, at http://www.dhs.gov/files/publications/gc_1281020492905.shtm#5.

[2] See TRACS PIA, DHS/NPPD/US-VISIT PIA-004, and TRACS SORN, DHS/NPPD/USVISIT-003, at http://www.dhs.gov/files/publications/gc_1281125467696.shtm#3.

[3] See ADIS PIA, DHS/NPPD/US-VISIT/PIA-005, and ADIS SORN, DHS/USVISIT-001, at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_adis_2007.pdf.

[4] If a subject has left the country, he or she may still be an overstay. However, the subject would not be an *in-country* overstay. Only in-country overstay leads are referred to ICE.

targeting rules. Once leads are confirmed and prioritized, US-VISIT refers this prioritized vetted overstay data to ICE for further investigation and possible enforcement action.

DHS anticipates expanding this pilot to a fully operational based on the outcome of this pilot phase. As changes are implemented that impact the privacy protections, this PIA will be updated.

Current Overstay Vetting Process

US-VISIT currently operates the Data Integrity Identity Validation (DIIV) system[5] to identify potential overstays based initially on information collected in ADIS. ADIS contains information about aliens who have applied for admission, entered, or departed the United States (U.S.). Using DIIV, US-VISIT generates a list of system-identified overstay leads and manually validates the leads. Once validated, US-VISIT prioritizes these leads according to existing ICE requirements and refers leads to ICE for further research and possible enforcement action. ICE conducts additional research to determine whether the individual is still in the U.S. and an actual overstay, whether the individual has departed the U.S. but the departure data was not collected or matched with the individual's record, or whether the individual adjusted his or her immigration status to that of a lawful permanent resident or otherwise applied for a change or extension of existing status with USCIS and is lawfully present. ICE uses these leads to deploy its investigative resources efficiently to locate high-risk overstays and initiate removal proceedings against them.

Previously, as part of the lead review process, US-VISIT would conduct three automated searches against other government systems on potential overstay. A record that could not be closed during those automated searches would then be manually validated through up to 12 federal systems. This process was time consuming, expensive, and led to a backlog of un-reviewed records.

In May 2011, DHS began a coordinated effort to vet all overstay leads against intelligence community and DHS holdings for national security and public safety concerns. In total, US-VISIT reviewed 1.6 million existing un-vetted overstay records and referred the vetted overstay leads to ICE for further investigation, indicating which may be criminal law enforcement and national security priorities.

One DHS Overstay Vetting Pilot Process

As part of the May 2011 effort, DHS learned that matching US-VISIT DIIV leads on a more frequent basis to additional data sets held by CBP eliminated misidentified leads because CBP held additional information indicating an individual's exit from the U.S. For example, a record that an individual applied for a visa from outside the U.S. at a date subsequent to his or her visa expiration date clarifies that the person has left the U.S. in the absence of departure data.

[5] DIIV is covered by the TRACS PIA and SORN. See footnote 2.

Additionally, CBP is able to run law enforcement and national security checks based on its established processes and rules to assist US-VISIT in prioritizing enforcement referrals to ICE. DHS established the Overstay Vetting Pilot to implement these improvements.

Initiation: US-VISIT to CBP and USCIS

During the Overstay Vetting Pilot, US-VISIT starts with its list of system-generated overstay leads from ADIS data. On a weekly basis, US-VISIT sends this file of leads to CBP via an encrypted email attachment or encrypted disc (when email is not possible). US-VISIT sends the same file of leads to USCIS via encrypted transmission (email attachment or encrypted disc when email is not possible). The lead file contains biographical information about the traveler including travel document identification number (e.g., passport number), date of birth, name, and country of citizenship.

Processing Results: CBP and USCIS to US-VISIT

CBP takes the US-VISIT file of leads and adds any matching data it finds from three types of data sets: 1) additional travel-related data, 2) criminal law enforcement and national security data; and 3) risk-based rules developed by analysts to assess and identify high risk travelers that may pose a greater risk of terrorist or criminal activity. CBP adds border crossing records from the Border Crossing Information system (BCI),[6] additional entry/exit data from the Form I-94 (retrieved from the Non-immigrant Information System (NIIS),[7] ICE Student and Exchange Visitor Information System (SEVIS) data,[8] and Department of State (DoS) Consular Consolidated Database (CCD) data.[9] CBP does not add any Passenger Name Records (PNR), which includes full travel itinerary, to this data set.

The criminal law enforcement and national security data added by CBP includes any hits generated by conducting name-based searches of individuals identified as a criminal or national security threat in the following databases: the Federal Bureau of Investigation's Terrorist Screening Database (TSDB) and National Crime Information Center (NCIC); and DHS/CBP TECS[10] national security, criminal, and public health lookouts.

---

[6] See Border Crossing Information SORN, DHS/CBP-007, at http://www.dhs.gov/files/publications/gc_1185458955781.shtm#3.

[7] See Non-immigrant Information System SORN, DHS/CBP-016, at http://www.dhs.gov/files/publications/gc_1185458955781.shtm#3

[8] See SEVIS PIA, DHS/ICE/PIA-001, and SEVIS SORN, DHS/ICE-001, at http://www.dhs.gov/files/publications/gc_1279833335485.shtm#0.

[9] See CCD PIA at http://www.state.gov/documents/organization/93772.pdf.

[10] See TECS PIA, DHS/CBP/PIA-011, at http://www.dhs.gov/files/publications/gc_1281020492905.shtm#8.

CBP also runs the last in-bound travel record of the US-VISIT lead file against risk-based rules. These rules are based on CBP officer experience, analysis of trends of suspicious activity, and raw intelligence from DHS and other government agencies. These rules are applied using the ATS Passenger (ATS-P) module of ATS, which provides selectivity and targeting capability to support CBP inspection and enforcement activities on air, ship, and rail travelers. If a lead hits on one of these rules, CBP adds a notation to the lead record indicating that lead matched a particular rule by providing a numeric code for the rule, but does not include any description of what the rule is.

CBP augments the US-VISIT lead file with its travel-related data, an indication that an individual matched a criminal law enforcement or national security data set, and if there is an indication that an individual matched a particular rule. CBP then sends it back to US-VISIT via encrypted email or disc. US-VISIT imports this data into a data file to remove duplicates then uploads the records into DIIV to process the new information from CBP. This process identifies those individuals who might not be considered overstays to reduce the manual processing necessary to validate the overstay record, and adds priority to those who hit against the lookouts contained in TSDB, NCIC, and/or TECS, or who hit against an ATS-P rule.

Similarly, USCIS runs the US-VISIT lead file against USCIS's CLAIMS 3 system, which contains information about immigration benefit applications and decisions. USCIS returns the immigration status data (to include pending, denied, approved) from CLAIMS 3[11] so that US-VISIT has recent immigration status updates on potential overstays in order to reduce the manual processing required.

Processing Results: US-VISIT to ICE

As part of the pilot, US-VISIT imports the pertinent data into DIIV for further review and analysis. US-VISIT removes all individuals who have left the country based on data received from CBP, USCIS, and an additional ADIS data pull. US-VISIT then manually validates all remaining leads to determine if there has been a subsequent arrival, departure, or change in immigration status that would place individuals in legal status, indicating that they are not an overstay. US-VISIT conducts this validation by performing manual searches against USCIS systems[12] as well as updated ADIS arrival and departure data. Individuals who remain overstay leads after the validation process are prioritized based on ICE requirements, any matches to criminal law enforcement and national security data, and matches to ATS-P rule(s). US-VISIT

[11] Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3). PIA and SORN for these systems are available by system title at http://www.dhs.gov/files/publications/gc_1279308495679.shtm.

[12] These systems include Person-Centric Query System, Central Index System, and Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3). PIAs and SORNs for these systems are available by system title at http://www.dhs.gov/files/publications/gc_1279308495679.shtm.

encrypts the spreadsheet of vetted and prioritized leads and sends it to ICE's Office of Homeland Security Investigations (HSI). The file contains the original biographic information from ADIS as well as the travel-related data, criminal law enforcement and national security data from CBP, and ATS-P rule identifier, if any. As part of this initial pilot, ICE will have access to the rule descriptions so that it can identify which CBP rules align with ICE enforcement priorities. ICE receives the encrypted file of vetted and prioritized leads via email and reviews the rule descriptions to manually identify priorities. This manual prioritization process is necessary for the initial pilot phase, but is expected to be automated in subsequent operational phases.

Once ICE has prioritized the leads according to its standards, a member of the HSI staff uploads all of the lead data into ICE's LeadTrac[13] system for further investigation and possible enforcement action. At the same time, ICE will send an encrypted email of the information to the National Counterterrorism Center (NCTC) for review and identification of terrorism information. If NCTC identifies a match between its records and those of overstay leads, it will notify ICE and maintain the matched record. For those records where there are no records, NCTC will retain the record for 180 days. For those leads where ICE has a need to know the individual's PNR or description of ATS-P rule as part of an active law enforcement investigation, designated HSI personnel may access that data directly via an active ATS-P user account. HSI personnel manually enter any relevant PNR data into LeadTrac on an individual basis. ICE may access the ATS-P rule description, but will not transfer the rule description into LeadTrac.

Privacy Risks and Mitigations

DHS recognizes that the potential privacy impact of mishandling this data is high. To mitigate overall privacy risks, the Privacy Office will conduct a Privacy Compliance Review (PCR) on this pilot within one year of its implementation (the date of this PIA) and/or before Overstay Vetting moves from a pilot phase to fully operational program.

Additionally, the Privacy Office identified four main privacy risks associated with conducting this pilot. These risks include security and accountability of extracted and duplicated data, risk of inaccurate or inappropriate data being attributed to a person via misuse of risk-based rules, risks to data integrity caused by the manual upload and transfer of data, and the risk to oversight and transparency because the LeadTrac PIA has yet to publish.

The process of transferring data extracts via email and/or disc introduces increased risk of loss and improper disclosure, and a process such as this occurring outside of a contained system circumvents built-in auditing mechanisms designed to detect and prevent data loss and misuse. To mitigate this risk, DHS has excluded certain highly sensitive PII, including full PNR and ATS-P rule descriptions, from being transferred via data extract. DHS is also planning

[13] See External Investigations SORN, DHS/ICE-009, available at http://www.dhs.gov/files/publications/gc_1185458955781.shtm#6. PIA for LeadTrac is pending.

modernization efforts to automate this process based on the outcome of this pilot, which will eliminate the need to manually transfer this data.

For data that is extracted and transferred during this pilot phase, US-VISIT transfers extracts via individual users' email accounts to ensure that the extract is going only to designated users (and their backups), and not to group accounts with multiple users. The emailed file is encrypted, and the password to open the file is never included in the same email transmission. Additionally, all *ad hoc* computer-readable extracts from ADIS, including extracts generated during this pilot, are manually logged by the ADIS system owner's internal chain of custody procedures, which ensure that the extract is reviewed every 90 days for necessity if not yet destroyed.[14] Extracts that remain in email files are further protected because they are within secured DHS local area networks. When the file cannot be emailed and must be transmitted via disc, the disc is encrypted and password sent by separate transmission, and the same chain of custody procedures and 90 day review occurs.

CBP takes the data extracts from US-VISIT and loads the information into ATS-P to conduct the matching against the CBP data sets and against scenario-based targeting rules. CBP destroys the data 90 days after receipt. CBP will track when the data was received, how many records were received, as well as when the results were provided to US-VISIT and ICE.

USCIS receives the extracted data from US-VISIT, reviews it to add any additional records USCIS may have in the CLAIMS 3 data, and returns the data extract with the additional information. The system-generated overstay leads are not maintained by USCIS after the processing is completed.

ICE HSI receives extracted data from US-VISIT during this pilot phase. To ensure accountability and security of these extracts, the HSI office that operates LeadTrac maintains a central log of all extracted data received from US-VISIT. The log captures the date and method of receipt, the date the data was uploaded into LeadTrac, and the date the original data file (email attachment or disc) was destroyed. The name of the HSI personnel who received, uploaded, and destroyed the incoming data is also noted on the log. HSI secures any data on portable media, such as disc, by keeping the data in a locked room or safe until it is destroyed. The HSI supervisor over this pilot project reviews the log regularly to ensure personnel are complying with the login procedures and that the data is being destroyed in accordance with the retention policy described in this PIA.

There is a risk that inaccurate or inappropriate assumptions about the individual could be attributed when information pertaining to the individual matches an ATS-P targeting rule. The rules are based on legal behaviors or characteristics that do not constitute reasonable suspicion of criminal or national security threat. Because these criteria do not constitute reasonable suspicion

[14] DHS Sensitive Systems Policy Documents (4300A)

of criminal law or national security violation, they are not appropriate for use in many contexts. These rules are appropriate for CBP because it is authorized to search without reasonable suspicion when an individual is crossing the border, and ICE may use these criteria for this pilot because it has first established reasonable suspicion that the individual is an overstay in violation of U.S. immigration law. Although appropriate for this pilot, there is a risk that this rule information could be misinterpreted if shared outside the context of this pilot. To mitigate this risk, CBP is not attaching a description of the rule to the vetted and prioritized lead's file that is transferred back to US-VISIT. Rather, US-VISIT only receives an identifier indicating which rule the individual hit upon, and any information about the rule remains in ATS-P to be accessed only by those ICE personnel trained to access and interpret that data. This risk is also mitigated by the fact that data on these rules are only referred to ICE if US-VISIT data supports reasonable suspicion that the individual has violated federal law by overstaying the terms of his or her admission.

The process of manually uploading data into each system rather than transferring it via system-to-system connections poses a risk to the integrity of the data, especially in the case of ICE's retrieval of PNR, which must be manually keyed into LeadTrac by ICE users based on their queries of ATS. This risk is mitigated by the training provided to all ICE law enforcement personnel on the conduct of investigations. ICE agents and officers are trained to manually compile case files and investigative analyses from various sources. HSI personnel who work in LeadTrac follow strict Standard Operating Procedures (SOPs) outlining how information is queried and manually recorded. ICE policies and training emphasize the importance of verifying the accuracy of information obtained from any secondary source before relying upon it to take a law enforcement action such as an arrest. The PNR entered into LeadTrac is used by ICE law enforcement officers solely to assist in investigations and not as evidence used directly to support an arrest, warrant, indictment, or prosecution. If PNR becomes necessary for evidentiary purposes in any particular investigation, prosecution, or other law enforcement matter, ICE law enforcement personnel would obtain the original PNR records either from the airlines via subpoena or from ATS-P.

Finally, the fact that the LeadTrac system is operating without a finalized PIA creates the risk of lack of oversight and transparency into the system. To mitigate this risk, ICE is allocating additional resources to prioritize and finalize the PIA during this pilot phase. It is anticipated that before this pilot moves into a fully operational phase, the LeadTrac PIA will have been approved and publicly available. The Privacy Office has also ensured that in the interim, the system is covered by the existing System of Records Notice (SORN) DHS/ICE-009 External Investigations and is fully integrated with the DHS Chief Information Security Officer's process for ensuring proper information security of DHS systems. This PIA also provides oversight and transparency into the system.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The legal authorities for the One DHS Overstay Vetting Pilot include: 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.

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 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 U.S.); 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); and 19 U.S.C. § 1509 (granting authority to take and consider evidence relating to Customs Duties).

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

This pilot uses information from several existing DHS record sources[15] to reduce misidentified leads and identify enforcement priority, including:

- DHS/NPPD/USVISIT-003 TRACS;
- DHS/USVISIT-001 ADIS;
- DHS/CBP-005 Advance Passenger Information System (APIS);
- DHS/CBP-006 ATS;

[15] Available at http://www.dhs.gov/files/publications/gc_1185458955781.shtm#3 under the relevant component

- DHS/CBP-007 BCI;
- DHS/CBP-009 Electronic System for Travel Authorization (ESTA);
- DHS/CBP-011 U.S. Customs and Border Protection TECS;
- DHS/CBP-016 Nonimmigrant Information System;
- DHS/ICE-001 SEVIS; and
- DHS/ICE-011 ENFORCE.

The vetted and prioritized leads are referred to ICE and become part of its DHS/ICE-009 External Investigations System of Records.

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

No. All participating systems (DIIV, ADIS, ATS, TECS, and LeadTrac) as well as the local area networks over which data extracts are transferred have approved system security plans and DHS is planning modernization efforts to automate this process based on the outcome of this pilot so that future efforts will be incorporated into a system security plan. In the interim, DHS is complying with DHS sensitive system security policy by logging and tracking these *ad hoc* computer-readable extracts and reviewing any remaining files every 90 days and adhering to audit and tracking controls residing in the systems from which manual transfers occur.

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

Yes. Overstay data is kept for 75 years in LeadTrac and DIIV in accordance with the NARA-approved schedule.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

This pilot is not collecting any additional information directly from the public and so is not covered by the PRA.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

Leads generated by US-VISIT DIIV are based on information collected from aliens who have applied for entry, entered, or departed the U.S. This information includes biographic data such as name, date of birth, travel document types and numbers, address, and context of the alien's encounter with the U.S. Government (e.g., border entry, immigration enforcement, or visa application).

US-VISIT transfers this data to CBP to add matching information about the alien from additional DHS travel data and data from other agencies available through ATS and TECS, which are fully described in the ATS and TECS PIAs. This data is all biographical and includes many data sets that may help US-VISIT determine if the alien who is the subject of the lead has actually exited the country and therefore is misidentified as a lead. Additional biographical and encounter data is added to determine enforcement priorities. This includes data on which leads, via a TECS search, hit against the TSDB, NCIC, or TECS national security, criminal, and public health lookouts, or who, via an ATS-P search, match an ATS-P rule. PNR data and rule descriptions are not included in the data sent back to US-VISIT.

The One DHS Overstay Vetting Pilot generates two additional data elements about an individual that is sent to ICE. The first is an indication that an overstay lead is vetted, indicating that known misidentified overstays have been eliminated from the lead file and remaining leads are suspected actual overstays based on an initial review of DHS data. The second additional piece of information is whether the individual is a law enforcement priority, and what type of priority the individual is. US-VISIT includes a project identifier in the data as a lead type so that ICE can categorize and prioritize the information based on current objectives. Only leads that meet HSI objectives are further reviewed and assigned to the field offices for investigations. All other leads that are not referred for criminal investigation are sent to ICE's Office of Enforcement and Removal Operations (ERO) for review and any appropriate administrative immigration related action.

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

Information comes from US-VISIT's ADIS and DIIV systems and is extracted and transmitted via encrypted transmission (either email or disc) to CBP and USCIS, which augment information about each lead based on data from ATS and TECS for CBP and CLAIMS 3 for USCIS. CBP and USCIS each transmit the original data along with additional matching data

back to US-VISIT DIIV via encrypted email or disc for US-VISIT analysts to remove misidentified leads and assign enforcement priority to vetted leads. US-VISIT then sends the vetted prioritized leads to ICE via encrypted email or disc, where ICE then uploads data into LeadTrac for further analysis and law enforcement case management.

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

This pilot does not introduce new uses of commercial or publicly available data. Existing US-VISIT and ICE processes permit use of commercial or publicly available data by a US-VISIT analyst or ICE law enforcement officer or analyst to compare information for accuracy. The data is never relied on as a primary source when making a decision about a law enforcement action against an individual.

2.4 Discuss how accuracy of the data is ensured.

A primary purpose of this pilot is to increase the accuracy of the existing overstay vetting process because of the inherent difficulty in determining whether an individual has left the country. Prior to this pilot, many individuals who had departed the U.S. but whose exit was not recorded by US-VISIT or whose exit data DHS was not to able match to entry information were misidentified as leads. By consulting additional data sources available via CBP, DHS is increasing the accuracy of the overstay leads sent to ICE by correcting the records of individuals misidentified as a lead. For USCIS data, the matching with immigration benefit data allows US-VISIT to identify when an individual has changed immigration status, and thus lawfully remain in the country.

Additionally, the pilot has built-in checks by trained DHS staff to ensure accurate interpretation of complex data sets. After CBP provides US-VISIT additional data on each lead, US-VISIT analysts process that information to determine the actual status and priority of each individual. Once the lead has been vetted and prioritized, it is handed to trained ICE criminal investigators and law enforcement officers to investigate each case on an individual basis.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of using ATS-P rules for purposes beyond their appropriate context via sharing those rules via this pilot.

Mitigation: ATS-P rules are based on legal behaviors or characteristics and threat-based scenarios that do not constitute reasonable suspicion of a criminal or national security threat. Because these criteria do not constitute reasonable suspicion of criminal law or national security violation, they are not appropriate for use in many contexts. These rules are appropriate for CBP

because it is authorized to search without reasonable suspicion when an individual is crossing the border, and ICE may use these criteria for this pilot because it has first established reasonable suspicion that the individual is an overstay.

Although appropriate for this pilot, there is a risk that this rule information could be misinterpreted if shared outside the context of this pilot. Therefore, DHS has taken measures to ensure the rule description is not attached to any information pertaining to the lead. Instead, only a unique identifier for the rule may attach to the lead during this pilot. As vetted and prioritized lead data is shared, the ATS-P rule will not be attached to the record.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

Biographic travel data is used in this pilot for two reasons: 1) to identify which vetted overstays are of greater priority for enforcement actions referred to ICE; and 2) to reduce misidentification of overstays. Immigration benefit data is used to identify individuals who have changed status and are lawfully present based on application or approval for such benefits. To reduce misidentified overstays, US-VISIT is matching this additional CBP, USCIS, and ICE biographic data against leads that may indicate the lead has left the country or is no longer violating his stay of admission. To identify enforcement priority, US-VISIT is matching lead data against existing CBP criminal law enforcement and national security risk lists and rules. Once leads are confirmed and prioritized, US-VISIT refers this prioritized overstay data to ICE for further investigation and any appropriate enforcement action.

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.

Yes. ATS-P processes traveller information against other information available to ATS, and applies threat-based scenarios comprised of risk-based rules. These rules were designed to assist CBP officers in identifying individuals who require additional inspection or in determining whether individuals should be allowed or denied entry into the United States. The risk-based rules are derived from discrete data elements, including criteria that pertain to specific operational or tactical objectives or local enforcement efforts. Unlike in the cargo environment, ATS-P does not use a score to determine an individual's risk level; instead, ATS-P compares information in ATS source databases against watch lists, criminal records, warrants, and patterns of suspicious activity or characteristics identified through past investigations and intelligence. The results of these comparisons are either assessments of the threat-based scenario(s) that a

traveller has matched, or matches against watch lists, criminal records, or warrants. Through this pilot, ICE will determine through this pilot whether it needs to refine or further focus those rules to improve the effectiveness of their enforcement activities.

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

NPPD US-VISIT, CBP, USCIS, and ICE staff are the only components with assigned roles in this pilot.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of using PNR data beyond its agreed upon purpose, as outlined in the 2007 US-EU PNR agreement.

Mitigation: To mitigate this risk, DHS has prohibited PNR data from being extracted in batch from ATS or sent via the pilot's process flow. Instead, ICE agents who have a specific need to know full PNR as part of an active law enforcement investigation may access PNR data by logging into ATS and viewing it via existing established processes.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

No additional data is collected directly from individuals as part of this pilot. Existing DHS data is used and shared in additional ways to reconcile misidentified leads and assign priorities for enforcement. This PIA provides notice of these new uses, as do the PIAs and SORNs for the underlying systems cited throughout this document. Additionally, individuals are aware that DHS maintains their travel data because in most cases they have provided it to DHS directly when crossing the border.

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

Individuals do not have the opportunity to consent to this specific use of their information.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: The LeadTrac system is operating without a finalized PIA, which creates

the risk of lack of oversight and transparency into the system.

Mitigation: To mitigate this risk, ICE is allocating additional resources to prioritize and finalize the PIA during this pilot phase. It is anticipated that before this pilot moves into a fully operational phase, the LeadTrac PIA will have been approved and publicly available. The Privacy Office has also ensured that in the interim, the system is covered by an existing SORN, DHS/ICE-009 External Investigations System of Records and is fully integrated with the DHS Chief Information Security Officer's process for ensuring proper information security of DHS systems. This PIA also provides oversight and transparency into the system.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

US-VISIT maintains data in DIIV for 75 years, including data processed and provided by CBP and USCIS. Extracts that exist outside of the IT system and that duplicate data in the system are deleted as soon as no longer required for pilot operations.

CBP maintains the US-VISIT lead data on the disc for 90 days and maintains the data in ATS-P only for the period of time it takes to process the data. CBP will track when the data was received, how many records were received, as well as when the results were provided to US-VISIT and ICE.

USCIS maintains the data extracts from the US-VISIT lead data as part of the email archive, the data that is run through the CLAIMS 3 database is not retained. The information is maintained in the email archive to provide an audit trail.

ICE maintains the LeadTrac records created based upon the US-VISIT-generated leads for 75 years from the date the lead record is closed in the LeadTrac system. The vetted lead data extracts obtained from US-VISIT is maintained by ICE in a secure electronic environment for five years in order to verify validity and to upload into LeadTrac, maintain the data for reference in the case of corruption or data integrity purposes, and for reporting purposes.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that data extracts may be retained longer than necessary because they are outside the control of the source system.

Mitigation: This risk is mitigated by the processes of logging and tracking data extracts, as established by NPPD US-VISIT, ICE, USCIS, and CBP, to ensure that extracts are accounted for and destroyed when no longer required.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state, and local government, and private sector entities.

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.

Yes, ICE will share the validated overstay leads with NCTC in order to identify terrorism information. ICE will send an encrypted with the overstay leads. NCTC will process the information and will retain any matches to its terrorism information and delete all other records 180 days after receipt.

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

DHS has entered into a new sharing agreement with NCTC in order to facilitate NCTC's counterterrorism efforts. This information sharing also aligns with DHS's mission to prevent and deter terrorist attacks. This sharing is conducted pursuant to routine use L of the DHS/ICE-009 External Investigations SORN, which states that DHS may share overstay lead information with "Federal and foreign government intelligence or counterterrorism agencies or components where DHS becomes aware of an indication of a threat or potential threat to national or international security, or where such use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure."

6.3 Does the project place limitations on re-dissemination?

Yes. The computer-readable extracts are controlled through a logging and destruction method. Within ATS-P, rule descriptions and PNR both have strict limits on re-dissemination within DHS, which is why both of these categories of records have been prohibited from being extracted from ATS and sent to other DHS systems via this pilot. Instead, designated ICE personnel with specific need-to-know may access that data by logging directly into ATS-P.

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

While this pilot does not introduce any disclosures of information outside of the Department, the process of having ICE log directly into ATS to access PNR on a vetted lead ensures that ICE will use the existing ATS process for logging disclosures of PNR outside of DHS. ICE officers log into ATS the fact that they brought PNR into LeadTrac and the specific authorized purpose(s) for doing so.

6.5 Privacy Impact Analysis: Related to Information Sharing

Not applicable, as this pilot does not introduce any sharing outside of DHS.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Certain information may be exempt from individual access because access to the data in underlying SORNs could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, or to the existence of the investigation, and could reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, or to avoid detection or apprehension. A determination whether a record may be accessed by the individual will be made at the time a request is received. DHS will review and comply appropriately with information requests on a case-by-case basis. An individual desiring copies of records maintained in this system should direct his or her request to the Freedom of Information Act (FOIA) Officer, US-VISIT Program, NPPD, U.S. Department of Homeland Security, Washington, D.C. 20528, or the ICE FOIA Office at (866) 633-1182 or visit the ICE FOIA Office's website (http://www.ice.gov/foia). The individual may also submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, Washington, D.C. 20528.

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

Individuals may have an opportunity to correct their data when it is originally collected; otherwise, they may submit redress requests. Because most of the data in DIIV is a copy of data provided by another system that originally collected the data, a redress request is most appropriately addressed to the originating system. If a correction is made to the information in

the original system, this new information will be available to DIIV in the same manner that it was originally available. An individual who is the subject of a record in this system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received. DHS will review and comply appropriately with information requests on a case-by-case basis. Requests for correction of records in this system may be made through the Traveler Redress Inquiry Program (TRIP) at www.dhs.gov/trip or via mail, facsimile, or e-mail in accordance with instructions available at www.dhs.gov/trip.

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

Notification is provided by the publication of this PIA and the published PIAs and SORNs for the underlying systems. In the case of redress requests for DHS organizations, if an individual is not satisfied with the response, the individual can appeal his or her case to the DHS Chief Privacy Officer, who will conduct a review and adjudicate the matter. Redress procedures are also noticed by the program through which the data was originally collected, and notification will vary based on that system.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk of insufficient redress available via this pilot because generally individuals are not directly able to access or correct their information.

Mitigation: Individual access in this context would interfere with the law enforcement purpose of the pilot and so is limited in this context. To mitigate the risk of inaccurate information, DHS will conduct a PCR on this pilot to ensure the PII involved is being handled according to the parameters outlined via this PIA.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

US-VISIT transfers computer-readable extracts via individual users' email accounts to ensure that the computer-readable extract is going only to designated users (and their backups), and not to group accounts with multiple users. The emailed file is encrypted, and the password to open the file is never included in the same email transmission. Additionally, all ad hoc computer-readable extracts from ADIS, including computer-readable extracts generated during this pilot, are manually logged by the ADIS system owner's internal chain of custody procedures, which ensure that the computer-readable extract is reviewed every 90 days for

necessity if not yet destroyed. Extracts that remain in email files are further protected because they are within secured DHS local area networks. When the file cannot be emailed and must be transmitted via disk, the disk is encrypted and password sent by separate transmission, and the same chain of custody procedures and 90 day review occurs.

Once extracted data is uploaded into systems with security authorizations, the existing security controls for those systems ensure that information is used in accordance with stated practices.

CBP will retain the computer-readable extracts provided by US-VISIT for a period of 90-days then the data is destroyed. CBP will track when the data was received, how many records were received, as well as when the results were provided to US-VISIT and ICE.

USCIS has a written procedure for handling the computer-readable extract that is received via encrypted email from US-VISIT. USCIS does not the load the information received from US-VISIT, but rather compares it to the information and then returns to US-VISIT any matches that it may find. The encrypted email is retained in the email system.

ICE has written procedures that govern the maintenance of the extracts received during this pilot and to ensure compliance with DHS security and privacy policies. The procedures require ICE to log all extracts received from US-VISIT, to store the data in an access restricted environment, and destroy the extract using appropriate secure deletion methods. HSI personnel who handle computer-readable extracts are trained on these procedures and the log is routinely reviewed by HSI supervisors to ensure compliance.

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

All DHS employees complete annual agency-managed privacy and security training, specifically the Culture of Privacy Awareness Training, Information Assurance Awareness Training and Basic Records Management Training. US-VISIT, CBP, and ICE employees also have taken the privacy training related to their use of CBP TECS, which requires users to complete a test successfully each year in order to maintain access to the system. CBP TECS access is required in order to access the other systems mentioned in this PIA and provides individuals additional awareness and training on handling PII.

At ICE, HSI personnel who handle extracts from US-VISIT are trained on HSI's procedures to log, track, secure, and ultimately destroy the computer-readable extract data according to the retention policy. Additional security and privacy training is provided to ICE field personnel throughout ICE.

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

In developing the DHS vetting overstay pilot, US-VISIT, CBP, USCIS, and ICE have identified a limited number of individuals who are authorized to receive the data as it is transmitted through encrypted disks and encrypted by email attachments. Once the data is loaded into the operational systems (i.e., ATS, DIIV, and LeadTrac), the existing user access controls are in place to ensure technically that system access is granted only to authorized users with a confirmed need to know based on their assignments and job responsibilities.

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?

For this pilot phase, no new uses will be introduced. When the current uses of information change, this PIA will be updated.

Responsible Officials

Diane Stephens, ADIS and IDENT Systems Owner, US-VISIT, NPPD

Thomas Bush, Executive Director, Targeting Division, Office of Intelligence and Investigative Liaison, CBP

Steven Cooper, Executive Director, Law Enforcement Information Sharing Initiative, ICE

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security