Privacy Impact Assessment Update
for the

Automated Targeting System

DHS/CBP/PIA-006(e)

January 13, 2017

Contact Point
Mario Medina
National Targeting Center
U.S. Customs and Border Protection
(202) 325-1251

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) operates the Automated Targeting System (ATS). ATS is a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based scenarios and assessments. CBP is updating this Privacy Impact Assessment (PIA) to notify the public about ATS user interface enhancements for passenger vetting (known as Unified Passenger or UPAX), the use of ATS for vetting new populations, vetting of master crew member list and master non-crew member list data collected under 19 CFR. 122.49c, and several new information sharing initiatives, including between the Transportation Security Administration (TSA) and CBP to enhance the identification of possible threats and to assist in securing the border and transportation security.

Overview

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) operates the Automated Targeting System (ATS) to facilitate legitimate trade and travel while managing the shared threat to the homeland posed by individuals and cargo that may require additional scrutiny prior to entering or exiting the United States. ATS supports CBP in identifying individuals and cargo that may require additional scrutiny across various transportation networks using the following functionalities:[1]

- Comparison: ATS compares information about travelers and conveyances arriving in, transiting through, or exiting the country against law enforcement and intelligence databases. For example, ATS compares information about individuals (identified as passengers, travelers, crewmembers, or persons appearing on documents supporting the movement of cargo) against the Terrorist Screening Database (TSDB)[2] as well as data concerning outstanding wants and warrants.
- Rules: ATS compares existing information about individuals and cargo entering and exiting the country with patterns identified as requiring additional scrutiny. The patterns are based on CBP Officer experience, trend analysis of suspicious activity, law enforcement cases, and raw intelligence.
- Federated Query: ATS allows users to search data across many different databases and systems to provide a consolidated view of data about a person or entity.

[1] For a complete overview of ATS, its modules, and the associated privacy risks, see DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update (June 1, 2012), *available at* https://www.dhs.gov/publication/automated-targeting-system-ats-update.

[2] ATS ingests the TSDB via the DHS Watchlisting Service (WLS). Please see DHS/ALL/PIA-027 Watchlist Service and subsequent updates for a full description of WLS, *available at* https://www.dhs.gov/publication/dhs-all-pia-027c-watchlist-service-update.

In order to execute the above three functionalities, ATS uses data from many different source systems. In some instances ATS is the official record for the information, while in other instances ATS ingests and maintains the information as a copy or provides a pointer to the information in the underlying system. Below is a summary; see Appendix A for referenced SORN citations.

- Official Record: ATS maintains the official record for Passenger Name Records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. § 44909, as implemented by 19 CFR 122.49d; for Importer Security Filing (10+2 documentation) and express consignment manifest information, which provides advanced information about cargo and related persons and entities for risk assessment and targeting purposes; for results of Cargo Enforcement Exams; for the combination of license plate, Department of Motor Vehicle (DMV) registration data, and biographical data associated with a border crossing; for certain law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information; and for certain information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department.
- Ingestion of Data: ATS maintains copies of key elements of certain databases in order to minimize the impact of processing searches on the operational systems and to act as a backup for certain operational systems, including, but not limited to: CBP's Automated Commercial Environment (ACE), Automated Commercial System (ACS), Overstay Leads from Arrival and Departure Information System (ADIS), Automated Export System (AES), Advance Passenger Information System (APIS), Border Crossing Information (BCI), Electronic System for Travel Authorization (ESTA), Electronic Visa Update System (EVUS), Global Enrollment System (GES), I-94 data, Non-Immigrant Information System (NIIS), Seized Asset and Case Tracking System (SEACATS), and TECS; the U.S. Citizenship and Immigration Services' (USCIS) Central Index System (CIS) data received through TECS, and special protected classes[3] data; the U.S. Immigration and Customs Enforcement's (ICE) Student Exchange and Visitor Information System (SEVIS) and Enforcement Integrated Database (EID), which includes Criminal Arrest Records and Immigration Enforcement Records (CARIER); Secure Flight Passenger Data (SFPD) and Master Crew List/Master Non-Crew List data from Transportation Security Administration (TSA); the Department of Justice's (DOJ) National Crime Information Center (NCIC) and Federal Bureau of Investigation (FBI) Interstate Identification Index (III) hits for manifested travelers; Electronic Questionnaires for Investigations Processing (e-QIP); historical National Security Entry-Exit Registration System (NSEERS); Flight Schedules and Flight Status

[3] Special protected classes of individuals include nonimmigrant status for victims of human trafficking, nonimmigrant status for victims of crimes, and relief for domestic violence victims.

OAG data; Social Security Administration (SSA) Death Master File; TSDB (Terrorist Screening Database), which ATS ingests from the WLS (Watchlist Service); and Non-immigrant and Immigrant Visa data from Department of State (DOS) Consular Consolidated Database (CCD), Refused Visa data from CCD, and the Consular Electronic Application Center (CEAC).

- Pointer System: ATS accesses and uses additional databases without ingesting the data, including: CBP's ADIS, Border Patrol Enforcement Tracking System (BPETS), Enterprise Geospatial Information Services (eGIS), e3 Biometrics System, and U.S. and Non-U.S. Passport Service through TECS; ICE's Enforcement Integrated Database (EID); DHS Automated Biometric Identification System (IDENT); USCIS's Person Centric Query System (PCQS); DOS CCD; commercial data aggregators; Nlets (not an acronym), DOJ's NCIC and the results of queries in the FBI's III; Interpol; the National Insurance Crime Bureau's (NICB's) private database of stolen vehicles.
- Data Manually Processed: ATS is used to manually process certain datasets to identify national security and public safety concerns and correlate records. Currently, DHS conducts this process for those records in ADIS that have been identified as individuals who may have overstayed their permitted time in the United States.

Reason for the PIA Update

ATS support for CBP's mission is directed into five general areas: 1) export of cargo; 2) import of cargo; 3) land borders; 4) air/sea borders; and 5) cross cutting view of risks across the four previous areas. To support these mission areas, ATS is divided into sub-systems or modules to support CBP Officers in determining whether or not a particular individual or cargo is higher risk than other individuals or cargo. Each sub-system uses slightly different data to conduct its risk assessment, but the basic purposes as described above remain the same. Previously issued PIAs for ATS discuss each module in detail and continue to apply unless otherwise specified in this document.[4]

Previously issued PIAs for ATS also discuss the scope of the targeting rules used by ATS. This process has not changed.[5] ATS continues to build risk-based assessments for cargo and conveyances based on criteria and rules developed by CBP. ATS maintains the assessment results from rules together with a record of which rules were used to develop the assessment results. With regard to travelers, ATS identifies persons whose information matches criteria comprising a targeting rule. This initial match and any subsequent matches are reviewed by CBP Officers to confirm continued official interest in the identified person. It is worth clarifying, however, that

[4] For a complete overview of ATS, its modules, and the associated privacy risks, see https://www.dhs.gov/publication/automated-targeting-system-ats-update.
[5] For a complete assessment of the rules process and procedures within ATS, please see the 2012 PIA for ATS: DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update (June 1, 2012), *available at* https://www.dhs.gov/publication/automated-targeting-system-ats-update.

only the ATS components pertaining to cargo or conveyances rely on rules-based targeting to build a score for the cargo or conveyance to subsequently identify cargo or conveyances of interest. Persons associated with cargo shipments are screened against TECS lookouts and prior law enforcement actions to permit any identified violations to be considered as part of the overall score. Travelers identified by risk-based targeting scenarios are not assigned scores.

ATS rules and assessment results from rules are designed to signal to CBP Officers that further inspection of a person, shipment, or conveyance may be warranted, even though an individual may not have been previously associated with a law enforcement action or otherwise be noted as a person of concern to law enforcement. ATS-Targeting Framework (TF) is a workflow and reporting function that separately allows users to track assessment results from rules and create various reports permitting a more comprehensive analysis of CBP's enforcement efforts.

ATS risk assessments are always based on predicated and contextual information. As noted above, unlike in the cargo and conveyance environments, ATS traveler risk assessments do not use a score to determine an individual's risk level; instead, they compare personally identifiable information (PII) from the databases listed above against lookouts and patterns of suspicious activity identified through past investigations and intelligence. This analysis is done in advance of a traveler's arrival in or departure from the United States and becomes one tool available to DHS officers in identifying illegal activity.

ATS modules support CBP's mission with the functionality summarized below, and described in more detail in previously published PIAs.

- Export Data: ATS evaluates export information, which includes information filed electronically with CBP. The export data is sorted, compared to rules, and scored so that CBP Officers can identify exports with transportation safety and security risks, such as Office of Foreign Assets Control (OFAC) violations, smuggled currency, illegal narcotics, and other contraband. ATS screens both commodity information on export documents and individuals identified on those documents. Officers can input findings from outbound exams of exports, generate multiple reports, and internally track shipments through custom rule criteria, review marking, and watched entity list.

- Inbound Cargo Screening: ATS evaluates all cargo to identify high risk inbound cargo for examinations. ATS uses rule and weight sets to analyze information from manifest, importer security filing, and entry data, to prioritize shipments for review and generate targets by scoring each shipment. In some places, ATS automatically places shipments on hold when they score above a specified risk threshold. ATS screens commodity information on the manifest, importer security filing, and entry data, and also screens individuals identified on these data sources against lookouts and prior violations.

- Vehicle and Traveler Targeting: ATS evaluates historical crossing records against internal and external data sources for targeting of vehicles and individuals at the border, as well as

for the identification of potential terrorists, transnational criminals, and in some cases, other persons who pose a higher risk of violating U.S. law. ATS is used within CBP by Passenger Analytical Units at Ports of Entry, the National Targeting Center (NTC), Border Patrol Agents, CBP headquarters intelligence analysts, and within DHS by DHS agents, analysts, and officers in the Office of Intelligence and Analysis (I&A), ICE, U.S. Coast Guard, and the TSA. ATS enables users to focus efforts on potentially high-risk passengers using a set of uniform and user-defined rules based on operational, tactical, intelligence, or local enforcement efforts.

- Non-Immigrant and Immigrant Visa and Visa Waiver Screening: ATS is used to vet non-immigrant and immigrant visa applications for DOS. DOS sends online visa application data to ATS-Passenger (ATS-P) for pre-adjudicative investigative screening, and ATS-P screens the visa application and provides a response to DOS whether or not derogatory information was identified by DHS about the individual. ATS also uses ESTA data to identify potential high risk applicants for the visa waiver program, and EVUS data to initially and recurrently vet applicants for 10-year multiple entry B1, B2, or B1/B2 visas. In addition, ATS uses information received from ADIS to identify individuals who may have overstayed the terms of their visas.

New ATS Privacy Impact Assessment Framework

CBP is conducting this PIA update to provide transparency and assess the privacy risks of several operational or enforcement programs. Due to the continuously changing threat environment in which CBP uses ATS, this PIA requires frequent, complex, and disparate updates. Therefore, CBP will conduct privacy risk assessments for each update as a separate "Update Addendum" to this PIA. As new changes or updates are required of ATS, CBP will issue additional Update Addendums to this PIA. Unless otherwise indicated in this document or future Addendums, the previously published ATS privacy compliance documentation continues to apply.

Responsible Officials

Mario Medina, Director, National Targeting Center
U.S. Customs and Border Protection
Department of Homeland Security

Debra L. Danisek, CBP Privacy Officer, Privacy and Diversity Office
U.S. Customs and Border Protection
Department of Homeland Security

Approval Signature

Original, signed copy on file at DHS Privacy

_____

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

ATS PIA Update Addendum Quick Reference Guide

ATS PIA Update Addendum 1:

Automated Targeting System-Passenger (ATS-P) – Module Updates

Last updated January 13, 2017 *(back to top)*

Automated Targeting System-Passenger (ATS-P) is a web-based enforcement and decision support tool used to collect, analyze, and disseminate information for the identification of potential terrorists, transnational criminals, and, in some cases, other persons who pose a higher risk of violating U.S. law. ATS-P capabilities are used at ports of entry to augment the CBP Officer's decision-making about whether a passenger or crew member should receive additional scrutiny.

ATS-P is also used within CBP by Passenger Analytical Units (PAU) at ports of entry, the National Targeting Center (NTC), Border Patrol Agents, CBP headquarters intelligence analysts, and within DHS by DHS agents, analysts, and officers in the Office of Intelligence and Analysis (I&A), ICE, U.S. Coast Guard, and TSA. ATS-P provides a hierarchical system that allows DHS personnel to focus efforts on potentially high-risk passengers by eliminating labor-intensive manual reviews of traveler information or interviews with every traveler. The assessment process is based on a set of uniform and user-defined rules based on specific operational, tactical, intelligence, or local enforcement efforts.

ATS-P is used to augment visa overstay leads received from Arrival and Departure Information Systems (ADIS) based on supporting data available in ATS (e.g., border crossing information, I-94 information, and Student and Exchange Visitor Information System (SEVIS) information). In addition to augmenting the list of overstay leads, ATS also develops priorities based on associated risk patterns. This prioritized list of overstay leads is then passed on to the LeadTrac case management system[6] for ICE to generate case leads.

By logging into ATS-P, authorized CBP and DHS personnel can access information from the various source systems on passengers who have arrived in and/or departed from the United States. ATS-P allows users to query other available Federal Government systems as well as publicly available information on the Internet through the user interface. In addition, ATS-P maintains a copy of information from the following systems: Advance Passenger Information System (APIS), I-94, Non-Immigrant Information System (NIIS), Electronic System for Travel Authorization (ESTA), Border Crossing Information (BCI), TECS secondary processing, and seizure and enforcement data, as well as Suspect and Violator Indices (SAVI), Central Index System (CIS), Electronic Visa Update System (EVUS), Global Enrollment Systems (GES), Terrorist Screening Database (TSDB) via the Watchlist Service, and the Department of State's (DOS) Consular Consolidated Database (CCD) Visa and Consular Electronic Application Center

[6] *See* DHS/ICE/PIA-044 LeadTrac System (July 22, 2016), *available at* https://www.dhs.gov/publication/dhsicepia-044-leadtrac-system.

(CEAC) data to identify individuals requiring additional scrutiny prior to entering or exiting the country.

Through the ATS-P web interface, authorized CBP personnel can create ad hoc queries on selected enforcement data, arrival and departure information, travel reservation information, visa and ESTA applications, and secondary referrals. Additionally, the ATS-P web interface may be displayed on approved mobile devices[7] to support officer activities in the context of the Immigration Advisory and Joint Security Programs (IAP/JSP) and at the ports of entry.

[7] This application was previously referred to as the Enforcement Link Mobile Operations (ELMO) mobile application, although now it is referred to as the "ATS Mobile application" following migration from the BlackBerry to the Android platform.

1.1 "Unified Passenger" (UPAX) Technology Update

January 13, 2017 *(back to top)*

ATS-P has traditionally served as a web-based enforcement and decision support tool used to collect, analyze, and disseminate information for the identification of potential terrorists, transnational criminals, and other persons who pose a higher risk of violating U.S. law. The CBP National Targeting Center (NTC) and ports of entry use ATS-P capabilities to augment a CBP Officer's decision-making about whether a passenger or crew member should receive additional inspection.

Unified Passenger (UPAX) is a technology refresh that updates and replaces the older functionality of the legacy ATS-P interface. This update allows ATS to process traveler information against other information available in ATS and apply risk-based rules centered around CBP Officer experience, analysis of trends of suspicious activity, and raw intelligence from DHS and other Government agencies. The end result is an improved process and system that assists CBP Officers in identifying individuals who require additional inspection and making admissibility decisions regarding individuals seeking admission to the United States. The updates to ATS involve a modernized visual presentation of relevant information used in the risk assessment process and a consolidation of multiple matched records and case management functions to ensure consistency and promote more efficient evaluation of potential risks. The enhanced presentation provided in the UPAX functionality provides direct access to cross-referenced files and information from partner agency databases through the use of hypertext links and single sign-on protocols. The system now integrates risk assessment and case management functionality with the presentation of query results across multiple source systems in a review of a traveler.

Specifically, the UPAX functionality unifies multiple possible match results from multiple source systems; reduces record duplication and streamlines the review process; standardizes the backend components under the CBP Target Technical Architecture to ensure consistency and improve maintainability and reusability; standardizes the entity resolution algorithms across all match results, providing improved consistency and maintainability as algorithm improvements are made and applied across the system; consolidates the front-end risk assessment components of ATS-P with the case management capabilities of the ATS-Targeting Framework (ATS-TF) under one user interface; and consolidates the query results across multiple source systems into an integrated view, including ATS-TF,[8] that eliminates the need for analysts to log into separate systems as they conduct their research.

[8] ATS-TF continues to exist as a separate module/sub-system within ATS, but UPAX provides the ability to create and manage TF events via the UPAX interface, which can be opened through the ATS-TF application.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

All of the authorities previously identified for ATS remain in effect. ATS derives its authority primarily from 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582; 8 U.S.C. § 1357; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347).

All previously identified SORNs remain in effect, or are noted under the "Notice" section below.

Characterization of the Information

Previously only available under ATS-TF, the UPAX module allows ATS-P users to track information of targeting interest regarding passengers and applicants for benefits or travel to the United States. Similar to ATS-TF, UPAX permits a user to search across the data sources available in the other modules of ATS based on role-based access for research and analysis purposes. If the user does not have access to the data, the search will not return any data. UPAX provides users with the ability to initiate research activities within the ATS-TF repository, fosters collaboration among analysts, and allows all users to use past activity logs as additional intelligence sources by tracking past research activity with respect to persons and entities of interest. UPAX includes workflow functionality, which allows authorized users to assign activities to other users, operating units, or ports of entry for additional processing. UPAX allows the creation of projects within the ATS-TF repository, which track information intended for use over long periods of time, or operational and analytical reports that may include public source information obtained by users for reference or incorporation into the report or project. Through the UPAX web interface, authorized CBP personnel can create ad hoc queries that allow users to find information related to a specific activity or entity contained within each activity. UPAX allows users to integrate data from multiple sources and show possible relationships between entities and data elements.

Users in UPAX may, subject to their access permissions, query the other four modules of ATS and other systems, including those noted below, and save the results:

- Border Patrol Enforcement Tracking System - Significant Incident Report (BPETS-SIR) Module - managed by CBP
- Enterprise Geospatial Information Services (eGIS) - managed by CBP
- TECS - managed by CBP

- Arrival and Departure Information System (ADIS) - managed by CBP
- U.S. and Non-U.S. Passports - managed by DOS and CBP
- Enforcement Integrated Database (EID) - managed by ICE
- Person Centric Query Service (PCQS) - managed by USCIS
- DHS Automated Biometric Identification System (IDENT) - managed by the DHS Office of Biometric Identity Management (OBIM)
- Watchlist Service - managed by DHS
- Consular Consolidated Database (CCD) - DOS
- Social Security Administration (SSA) Death Master File - managed by SSA (a copy of this file is kept in ATS-TF)
- National Crime Information Center (NCIC) - managed by Department of Justice (DOJ)
- Interpol Lost/Stolen passports
- Nlets
- Commercial data aggregators

UPAX also allows authorized users to attach public source information, such as responsive Internet links and related documents, to an assigned report and/or project and search for any text contained within the system via full text search functionality. UPAX also includes sophisticated ad hoc reporting features for both system data and workflow metrics as well as initial reporting features through data warehouse capabilities.

There are no new privacy risks regarding characterization of information related to CBP's ATS-P UPAX enhancement. UPAX permits users to view a consolidated profile of a passenger by displaying records from multiple systems as part of one UPAX record. This eliminates the need for CBP Officers to view records from multiple systems with multiple log-on information. Because UPAX does not permit users to access any new information, but rather displays existing information in a more efficient manner, and because UPAX only permits a user to search across the data sources available in the other modules of ATS based on role-based access for research and analysis purposes, there are no new privacy risks.

Uses of the Information

The UPAX functionality unifies multiple possible match results from multiple source systems; reduces record duplication and streamlines the review process; standardizes the backend components under the CBP Target Technical Architecture to ensure consistency and improve maintainability and reusability; standardizes the entity resolution algorithms across all match

results, providing improved consistency and maintainability as algorithm improvements are made and applied across the system; consolidates the front-end risk assessment components of ATS-P with the case management capabilities of the ATS-TF under one user interface; and consolidates the query results across multiple source systems into an integrated view, including ATS-TF, that eliminates the need for analysts to log into separate systems as they conduct their research.

Privacy Risk: There is a privacy risk to use limitation due to the consolidation of multiple datasets and query results in one system.

Mitigation: This risk is mitigated through role-based access controls. User roles are restricted and audited, with access predicated on "need to know." Through user access control "entitlements," all ATS users are only permitted to access information from the source systems to which they have already been granted access through supervisory approval.

Privacy Risk: There is a privacy risk to data integrity because CBP analysts are relying on aggregated information, which may become stale or inaccurate since pulled from source systems.

Mitigation: This risk cannot be fully mitigated. CBP relies upon the source systems to ensure that data ingested by ATS is accurate and complete. Discrepancies may be identified in the context of a CBP Officer's review of the data, and CBP Officers are required by policy to take action to correct the data if they become aware of inaccurate data, when appropriate. For Passenger Name Records (PNR), CBP Officers may become aware of inaccuracies due to correction, rectification, or redress procedures available to travelers, including non-U.S. persons. Although ATS is not the system of record for most of the source data, ATS receives updates with any changes to the source system databases. Continuous source system updates occur in real-time or near real-time. When corrections are made to data in source systems, ATS updates this information immediately and only the latest data are used. In this way, ATS integrates all updated data (including accuracy updates) in as close to real-time as possible.

To the extent information that is obtained from another government source (for example, vehicle registration data that is obtained through Nlets) is determined to be inaccurate, this problem would be communicated to the appropriate government source by the CBP Officer for remedial action.

Notice

CBP is conducting this PIA update to provide notice of the ATS-P UPAX technology refresh. There are no new privacy risks to notice identified with this enhancement.

Data Retention by the project

During this privacy impact assessment process, CBP determined that ATS is retaining ingested information consistent with its own 15-year retention period, as opposed to the source system records retention period. As described in previously published PIAs, to the extent information is ingested from other systems, data should be retained in ATS in accordance with the

record retention requirements of those systems, or the retention period for ATS, whichever is shortest. The retention period for the official records maintained in ATS will not exceed 15 years, after which time the records will be deleted, except as noted for PNR.

Privacy Risk: There is a risk that ATS will retain all ingested records for targeting purposes for 15 years, regardless of the source system data retention requirements.

Mitigation: CBP Privacy is developing a mitigation strategy for this risk. Understanding that the justification for a 15-year retention period for the official records is based on CBP's law enforcement and security functions at the border, CBP must balance the need for historical data for targeting purposes with the original purpose of collection and public notices already provided about the ingested data. The ATS 15-year retention period is based on CBP's historical encounters with suspected terrorists and other criminals, as well as the broader expertise of the law enforcement and intelligence communities. It is well known, for example, that potential terrorists may make multiple visits to the United States in advance of performing an attack. It is over the course of time and multiple visits that a potential risk becomes clear. Travel records, including historical records, are essential in assisting CBP Officers with their risk-based assessments of travel indicators and identifying potential links between known and previously unidentified terrorist facilitators. Analyzing these records for these purposes allows CBP to continue to effectively identify suspect travel patterns and irregularities.

CBP Privacy will conduct a CBP Privacy Evaluation (CPE) on the retention process and data tagging for retention purposes within ATS for all source datasets within one year of publication of this PIA. Following the CPE, CBP Privacy will make recommendations regarding changing or modifying the underlying source system retention period to better align with CBP operational needs, or will require a process by which ATS follows the underlying source system retention periods. The results of the CPE will be shared with the DHS Privacy Office.

Information Sharing

As noted above, ATS does not consistently follow source system retention periods, but instead relies on the ATS-specific retention period of 15 years. Due to the nature of many CBP large, legacy, transactional databases, most information sharing is done via a connection to ATS. Therefore, it is likely that information shared from ATS to other partners may also be retained in a manner that is inconsistent with the original source systems.

Privacy Risk: There is a privacy risk to information sharing because ATS may retain information longer than the source system data retention requirements, and therefore may pass data to partners that should no longer be held by CBP.

Mitigation: This risk is partially mitigated. Bulk information sharing agreements are covered by their own, specific information sharing access agreements (ISAA), such as a Memorandum of Understanding (MOU), which typically detail a records retention requirement tailored to that specific agreement consistent with CBP retention requirements. As part of the CBP

Privacy Evaluation regarding the retention issues in ATS, CBP Privacy will also conduct a review of the ISAAs implicating CBP data to determine if: a) ATS is used as the conduit for transmission, and b) if the transmission of information is consistent with the underlying source data retention requirements.

Redress

There are no changes to redress from previously issued ATS PIAs.

Auditing and Accountability

The auditing and accountability procedures for UPAX are enhanced from previous technology updates to ATS-P. UPAX performs more granular auditing in terms of vetting performed by a user, in which each derogatory record is marked with individual vetting results. ATS-P allowed the disposition to be set at the higher level, but not per individual. UPAX marks the vetting results at a more granular level, which is more accurate, and retains records of all user search and vetting results.

1.2 Facial Recognition Technology Update

January 13, 2017 *(back to top)*

Currently, CBP checks all incoming passengers biographically against the FBI's National Crime Information Center (NCIC) and Criminal Master File for subjects who may have criminal activity that would prohibit their admission or indicate they are wanted for suspected and/or actual criminal activity. Additionally, those individuals subject to biometric capture are checked against the DHS Automated Biometric Identification System (IDENT)[9] and in some instances, the FBI's Next Generation Identification/Integrated Automated Fingerprint Identification System (NGI/IAFIS)[10] containing criminal history information using name and date of birth and/or fingerprints to check for subjects who may have criminal activity that would prohibit their admission or indicate they are wanted for suspected and/or actual criminal activity.

Under this initiative, CBP will use ATS to search the FBI's NGI Interstate Photo System (IPS), which contains all photos received by the FBI with ten print criminal booking transactions, using photographs from:

1) TECS;[11]
2) Department of State's (DOS) Consular Consolidated Database (CCD);[12]
3) USCIS' Biometric Storage System (BSS) or Person Centric Query System (PCQS);[13]
4) IDENT; and
5) Global Enrollment System (GES)[14] for travelers that are of national security interest to CBP.

CBP is able to share DOS information with the FBI since DOS is a party to the 2008 DHS-DOJ/FBI-DOS Memorandum of Understanding (MOU) to share biographic and biometric information and as reflected in relevant technical documents.

---

[9] *See* DHS/USVISIT-004 DHS Automated Biometric Identification System (IDENT), 72 FR 31080 (June 5, 2007), *available at* https://www.gpo.gov/fdsys/pkg/FR-2007-06-05/html/07-2781.htm.
[10] *See* DOJ/FBI-009 Fingerprint Identification Records System (FIRS), 72 FR 3410 (January 25, 2007), *available at* https://www.gpo.gov/fdsys/pkg/FR-2007-01-25/pdf/E7-1176.pdf.
[11] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008, *available at* https://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm.
[12] *See* Consular Consolidated Database (CCD) (July 17, 2015), *available at* https://www.state.gov/documents/organization/242316.pdf.
[13] *See* DHS/USCIS-003 Biometric Storage System, 72 FR 17172 (April 6, 2007), *available at* https://www.gpo.gov/fdsys/pkg/FR-2007-04-06/html/07-1643.htm.
[14] *See* DHS/CBP-002 Global Enrollment System, 78 FR 3441 (January 16, 2013), *available at* https://www.gpo.gov/fdsys/pkg/FR-2013-01-16/html/2013-00804.htm.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

All of the authorities previously identified for ATS remain in effect. ATS derives its authority primarily from 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582; 8 U.S.C. § 1357; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347).

All previously identified SORNs remain in effect, or are noted under the "Notice" section below.

Characterization of the Information

The photographs of individuals and/or associates that match information indicating a national security concern and the associated personally identifiable information (PII) (including: Place of Birth, Country of Citizenship, Date of Birth, Age Range, Sex, Race, Scars/Marks/Tattoos, Height Range, Weight Range, Eye Color, Hair Color) will be passed via ATS to IDENT and forwarded to the FBI's NGI IPS for a search and a response of candidate photographs. IDENT will serve as a pass-through only; therefore it will not store either the request message or the responses. An individual's photograph would be transmitted from ATS to IDENT and then to FBI's NGI because IDENT already has an interface to NGI, whereas ATS does not.

Search results are generated automatically by the FBI facial recognition software (no human intervention by the FBI) and returned in a ranked candidate list of no more than three candidates. There is no "match rate" because the FBI does not provide "matches" but rather provides potential candidates and CBP will determine whether there is a match. The search will only include the FBI NGI IPS and no information would be retained by the FBI. The candidate photographs will then be returned to IDENT and passed back to ATS, at which point CBP Officers and analysts will use the candidate images and all other available information to CBP for identity resolution purposes to determine if there is a confirmed match as well as review, analyze, and conduct further research on these individuals.

Privacy Risk: There is a privacy risk of over-collection since CBP will collect and retain photographs of individuals who are potential matches to subjects of national security interest.

Mitigation: For possible matches returned by the FBI, CBP may retain these photographs consistent with other law enforcement or national security leads in ATS. However, to ensure no

needless collection while meeting law enforcement needs, CBP will only retain the possible matches for 31 days to permit CBP time to conduct further analysis to make a determination, while limiting the time possible matches (or candidates) may be stored to protect the privacy interests. While most determinations could be made in a shorter period, the 31 days may be necessary to collect additional information from other sources, such as Government agencies to complete final identity determinations, if necessary and appropriate. CBP, through ATS, will document the requirement for deletion of possible matches within 31 days in its internal requirements tracking system and will set up a mechanism within ATS to delete the possible matches within this time frame. Once a photograph has been determined a non-match, it will be deleted within the 31-day period.

Privacy Risk: There is a privacy risk to data integrity due to the potential imprecision of automated facial recognition technology.

Mitigation: CBP Officers and analysts will receive FBI training on facial recognition to assist with the match determination. The confirmed matches, which are linked to a national security concern, would be retained in ATS-TF consistent with the ATS retention schedule. The confirmed match photos will be maintained in ATS-TF as an official record of ATS. CBP Officers and analysts will also use all other information available to them to make a match determination, so that a match is not solely based on the facial recognition technology.

Uses of the Information

CBP may use the FBI's facial recognition software to assist in targeting and identity resolution, consistent with the ATS System of Record Notice (SORN).[15] The ATS SORN permits CBP's use of information to "perform targeting of individuals who may pose a risk to border security or public safety, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law" or "to otherwise assist in the enforcement of the laws enforced or administered by DHS, including those related to counterterrorism." All individuals whose photographs are submitted to the FBI are already of national security concern to CBP.

Consistent with that purpose, CBP may collect information about any type of individual identified under the ATS SORN for vetting purposes. CBP may collect and store the potential matches from the FBI under the "G. Persons whose data was received by the Department as the result of memoranda of understanding or other information sharing agreement or arrangement because the information is relevant to the border security mission of the Department" and "I. Persons who may pose a threat to the United States" categories of individuals.

Lastly, ATS is permitted to store biometrics, such as photographs, consistent with the ATS SORN.

[15] *See* DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012), *available at* https://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm.

Privacy Risk: There is a privacy risk to use limitation that information sent to or returned from the FBI based on the facial recognition technology will be stored or enrolled in IDENT and then accessed by other Departments or agencies that have access to IDENT.

Mitigation: IDENT will be used only as a pass-through to FBI NGI; it will not store any of the query data or returned results from NGI. CBP Privacy will conduct a CBP Privacy Evaluation (CPE) within one year to verify that IDENT is not storing the query or retuned results. The results of the CPE will be shared with the DHS Privacy Office.

Privacy Risk: There is a privacy risk that individuals who submit their photographs to DOS for an immigration or non-immigrant benefit will be unaware that their photos will be shared between the FBI and DHS for facial recognition purposes.

Mitigation: Consistent with the relevant DOS SORNs, DOS shares biometric and biographic data with DHS for vetting as part of its standard adjudication process. Use of facial recognition technology is another vetting technique. DHS is currently updating the existing MOU with DOS to clarify the updated biometrics modalities used for vetting.

Notice

CBP is conducting this PIA update to provide notice of CBP's use of FBI Facial Recognition Technology.

Privacy Risk: There is a privacy risk to notice that individuals who submit photographs to DOS will be unaware of DHS's use of FBI facial recognition technology to conduct matches.

Mitigation: This PIA provides notice of the sharing of this data for the purposes outlined above and consistent with restrictions and safeguarding of such data that is required by law and DHS policies. In addition, the DOS PIA for CCD provides notice that CCD information is shared with OBIM and CBP.[16]

Data Retention by the project

For CBP's use of the FBI Facial Recognition Technology, CBP passes photographs and certain PII via ATS to IDENT, which is then forwarded to the FBI's NGI IPS for comparison. When NGI IPS identifies three candidates for the photograph that was sent, FBI will pass back photograph(s) and the associated Controlling Agency Identifier (referred to by the FBI as the Universal Control Number, or UCN).

Privacy Risk: There is a risk that the FBI will retain information from CBP for its own query purposes.

[16] *See* Privacy Impact Assessment, Consular Consolidated Database (July 17, 2015), *available at* https://foia.state.gov/_docs/PIA/ConsularConsolidatedDatabase_CCD.pdf.

Mitigation: Pursuant to the requirements of the information sharing agreement, the FBI will not retain the information that was queried.

Privacy Risk: There is a risk that CBP will retain the potential matches or other gallery images that have no nexus to national security.

Mitigation: The confirmed matches, which are linked to a national security concern, would be retained in ATS-TF consistent with the ATS retention schedule. CBP may retain the possible matches for up to but not longer than 31 days to conduct further analysis to make a determination. However, once a determination is made, the photographs that do not match will be deleted.

Information Sharing

There are no changes to information sharing from previously issued ATS PIAs.

Redress

Although there are no changes to information sharing from previously issued ATS PIAs, for this initiative, there is a risk that two types of individuals will be unable to achieve redress in the event of an incorrect match: (a) individuals who submit photographs to DOS, and (b) individuals who are false-positive potential matches.

Privacy Risk: Individuals whose information is submitted to CBP from DOS or the FBI may be unable to achieve redress or determine which Government procedures are appropriate to assist them.

Mitigation: This risk is mitigated, to extent possible consistent with law enforcement and national security exemptions noted in the applicable SORNs. To the extent that a record is exempted in a source system, the exemption will continue to apply.

A traveler, regardless of his or her citizenship or residence, may obtain access to his or her PNR. However, records concerning the targeting rules, the responses to rules, case events, law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information, information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department, or records exempted from access by the system from which ATS ingested or accessed the information will not be accessible to the individual.

Notwithstanding the applicable exemptions, CBP reviews all such requests on a case-by-case basis. If compliance with a request would not interfere with or adversely affect the national security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of CBP in accordance with procedures and points of contact published in the applicable SORN.

Procedures for individuals to gain access to data maintained in source systems that provide data ingested into ATS are covered by the respective SORNs for the source systems. Individuals

may follow the procedures outlined in the PIAs and SORNs of the source systems to gain access to their information stored in those systems.

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a Freedom of Information Act (FOIA) or Privacy Act request in writing to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, D.C. 20229

FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Specific FOIA contact information can be found at http://www.dhs.gov/foia under contacts.

If a traveler believes that CBP actions are the result of incorrect or inaccurate information, then inquiries may be directed to:

CBP INFO Center
OPA—Rosslyn
U.S. Customs and Border Protection
1300 Pennsylvania Avenue NW
Washington, D.C. 20229

Travelers may also contact DHS TRIP, 601 South 12th Street, TSA-901, Arlington, VA 22202 or online at www.dhs.gov/trip. Individuals making inquiries may be asked to provide additional identifying information to enable DHS to identify the record(s) at issue.

Auditing and Accountability

For possible matches, CBP may retain these photographs consistent with other law enforcement or national security leads in ATS. However, to balance the privacy interests and law enforcement needs, CBP will only retain the possible matches for 31 days to permit CBP time to conduct further analysis to make a determination, while limiting the time possible matches (or candidates) may be stored to protect the privacy interests. While most determinations could be made in a shorter period, the 31 days may be necessary to collect additional information from other sources, such as Government agencies to complete final identity determinations, if necessary and appropriate. CBP, through ATS, will document the requirement for deletion of possible matches within 31 days in its internal requirements tracking system and will set up a purge mechanism within ATS to delete the possible matches within this time frame. Once a photograph has been determined a non-match, it will be deleted within the 31-day period.

1.3 Transportation Security Administration (TSA) Secure Flight Passenger Data (SFPD) Vetting

January 13, 2017 *(back to top)*

CBP will now ingest TSA Secure Flight Passenger Data (SFPD) in real time into ATS-P for the following two types of flights:

(1) U.S. and foreign air carriers that fly over the United States (i.e., overflights), but never touch down into the United States, such as flights from Mexico to Canada.

(2) U.S. carriers that fly from one international point to another international point (i.e., point-to-point flights), such as Berlin to Shanghai.

TSA's Secure Flight program screens aviation passengers and certain non-travelers before they access airport sterile areas or board aircraft. TSA has conducted several thorough PIAs[17] and a SORN[18] regarding the Secure Flight program. Unless otherwise noted, the information provided in previously published TSA Secure Flight PIAs remains in effect. Individuals are encouraged to read all program PIAs to fully understand TSA's privacy assessment of the Secure Flight program.

The Secure Flight regulation[19] requires foreign and U.S. air carriers to submit SFPD for covered flights for each travel reservation. SFPD includes: 1) full name, 2) date of birth, 3) gender, and, if available, 4) Redress Number and Known Traveler number, 5) passport information (if applicable), 5) reservation control number, 6) record sequence number, 7) record type, 8) passenger update indicator, 9) traveler reference number, and 10) itinerary information.[20] ATS will ingest all of the data elements collected by TSA and authorized through the Secure Flight regulation for the two types of flights mentioned above.

Background

Since inception, CBP and TSA have both played a role in pre-flight screening and risk assessments. But there are some major differences between the TSA Secure Flight process and CBP's collection of advanced passenger information. Under the Secure Flight program, covered aircraft operators must request passenger information at the time of reservation or prior to transmitting the passenger's SFPD; CBP requires the electronic transmission of manifest information for passengers and crew members onboard commercial and private aircraft, in advance of arrival in and departure from the United States, and for crew members and non-crew members

[17] *See* DHS/TSA/PIA-018 Secure Flight Program, and subsequent updates, *available at* https://www.dhs.gov/publication/dhs-tsa-pia-018g-secure-flight-program-update.
[18] *See* DHS/TSA-019 Secure Flight Records, 80 FR 233 (January 5, 2015), *available at* https://www.gpo.gov/fdsys/pkg/FR-2015-01-05/html/2014-30856.htm.
[19] 49 CFR 1560.101(b).
[20] 49 CFR 1560.3. "Covered flights" are defined in the Secure Flight regulation at 49 CFR 1560.3 and include overflights and international point-to-point flights by U.S. carriers.

onboard commercial aircraft that overfly the United States in advance of the departure of those flights. TSA requires collection of different data elements under the Secure Flight program than CBP collects under the Advance Passenger Information System (APIS) regulations.[21] Covered aircraft operators can transmit both APIS data and SFPD in a single transmission to the DHS portal, which will route information to TSA and CBP accordingly.[22]

Covered aircraft operators must submit this SFPD information approximately 72 hours before departure of a covered flight, or if a passenger books after this 72-hour mark, as soon as that information becomes available. Those that elect to transmit the SFPD and all manifest information required under the APIS regulations at the same time would be able to send a single transmission to DHS.

Pre-Screening Program

ATS provides a pre-screening service to TSA to enhance the security of international air travel by identifying individuals who present security concerns. TSA provides risk-based, intelligence-driven, scenario rules to CBP for use in ATS to identify international travelers requiring enhanced screening. Individuals identified through this program are subjected to Selectee screening prior to boarding an aircraft. While passenger data for international incoming flights (flights from a foreign airport to a U.S. airport) are pre-screened, this program is not applied to SFPD because ATS does not receive such data. However, TSA does receive this information.

To apply this program to these overflight and point-to-point flights, the SFPD will now be ingested into ATS so that ATS is able to match the criteria in the rules against the SFPD. TSA would then be able to identify individuals who, though not on a watch list, exhibit high risk indicators or travel patterns, and thus should be subject to Selectee screening.[23] Having CBP perform a pre-screening service for these covered flights supports its border security mission and could aid in tracking travel of individuals in situations such as those presented by a communicable disease outbreak (such as the Ebola outbreak).

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

[21] *See* Secure Flight Final Rule, 73 FR 64023 (October 28, 2008) for a table delineating SFPD and APIS Pre-Departure data elements, *available at* https://www.federalregister.gov/documents/2008/10/28/E8-25432/secure-flight-program.
[22] Covered aircraft operators may also submit Passenger Name Record information to CBP through this DHS portal.
[23] Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) § 4012(a) (Pub. L. 108-458, 118 Stat. 3638, December 17, 2004). Currently, the consolidated and integrated terrorist watch list is maintained by the FBI's Terrorist Screening Center (TSC) in the Terrorist Screening Database (TSDB). The No Fly and Selectee List are components of the TSDB.

All of the authorities previously identified for ATS remain in effect. ATS derives its authority primarily from 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582; 8 U.S.C. § 1357; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347). See also, e.g., 6 U.S.C. §§ 111, 211; 8 U.S.C. §§ 1103, 1182, 1225, 1225a, 1324, 1357; 19 U.S.C. §§ 1431, 1433, 1436, 1448, 1459, 1590, 1594, 1623, 1624, 1644, and 1644a.

All previously identified SORNs remain in effect, or are noted under the "Notice" section below.

Characterization of the Information

CBP will now ingest SFPD in real time from the DHS Router into ATS-P for the following two types of flights:

- U.S. and foreign air carriers that fly over the United States (i.e., overflights), but never touch down into the United States, such as flights from Mexico to Canada.
- U.S. carriers that fly from one international point to another international point (i.e., point-to-point flights), such as Berlin to Shanghai.

CBP is ingesting the following data elements from TSA: 1) full name, 2) date of birth, 3) gender, and, if available, 4) Redress Number and Known Traveler number, 5) passport information (if applicable), 5) reservation control number, 6) record sequence number, 7) record type, 8) passenger update indicator, 9) traveler reference number, and 10) itinerary information. These data elements are currently collected under current TSA procedures and authorized through the TSA Secure Flight regulation.

Privacy Risk: There is a risk of over-collection and a risk to purpose specification since the SFPD is originally collected by TSA.

Mitigation: CBP has authority to receive SFPD overflight and point-to-point flight information from TSA for purposes of assisting TSA and to enhance CBP's mission pursuant to the authorities mentioned above.

CBP's systems will retain the above referenced SFPD of individuals for a period of time consistent with (and in some cases, shorter than) the Secure Flight records retention schedule. For individuals who do not match to information indicating a potential risk (i.e., non-matches), these records will be held for 7 days to create, modify, and run rules, as well as to conduct additional analysis on the data.[24] After 7 days, the records will be deleted from ATS. This category should be the majority of the SFPD records.

[24] This retention period is consistent with the DHS/TSA-019 Secure Flight SORN.

CBP relies on ATS to maintain records of individuals who were: 1) confirmed as watchlist matches (15-year retention), 2) possible watchlist matches who are subsequently cleared (7-year retention), and 3) rule hits (7-year retention). However, data that is linked to a border security, national security, significant health risk, or counterterrorism matter will be retained in ATS for the life of the matter to support that activity and other similar activities that may become related.

CBP relies on TECS[25] to maintain records about those individuals who may need additional scrutiny when entering the country. Possible matches and rule matches will be retained consistent with the TSA retention schedule and confirmed Watchlist Lookouts will be retained for 75 years. However, data that is linked to a border security, national security, significant health risk, or counterterrorism matter will be retained in TECS for the life of the matter to support that activity and other similar activities that may become related.

Uses of the Information

CBP will use the information to:

1) match the SFPD data against the Terrorist Screening Database (TSDB);

2) display the data within ATS and on the TSA-CBP Common Operating Picture;

3) update the Terrorist Identities Datamart Environment (TIDE) and the TSDB;

4) submit new watchlist nominations; or

5) other appropriate uses which enhance CBP's border security mission.

These actions provide better information to appropriate U.S. authorities (including CBP and TSA) receiving such information to assist in identifying individuals of potential concern. Finally, the information is critical in case a flight overflying the United States has to make an emergency landing in the United States. In such a situation, CBP needs information immediately about who is on that flight.

Consistent with the purposes for which the Secure Flight program was created, TSA has authorized CBP to use the SFPD for border security, counterterrorism, significant health threat (e.g., pandemic), and national security purposes.

Privacy Risk: There is a risk that CBP will use SFPD for purposes beyond border security, national security, significant public health risk, and counterterrorism, such as for law enforcement purposes.

Mitigation: TSA and CBP have worked together on processes and procedures in place to ensure the data is properly being used. CBP Privacy will conduct a CBP Privacy Evaluation (CPE)

[25] *See* DHS/CBP-011 TECS, 73 FR 77778 (December 19, 2008), *available at* https://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm.

within 6 months of CBP beginning regular ingest of the SFPD to evaluate these risks and mitigations. The results of the CPE will be shared with the DHS Privacy Office.

Privacy Risk: There is a risk that CBP will use SFPD to generate new targeting rules without appropriate oversight.

Mitigation: CBP will follow its current policy regarding the existing DHS oversight mechanism to ensure that targeting rules align with DHS policies. In addition, CBP Privacy will conduct a CPE within 6 months of CBP beginning regular ingest of the SFPD to evaluate these risks and mitigations. The results of the CPE will be shared with the DHS Privacy Office.

Notice

TSA has provided extensive notice about the Secure Flight program in general, including a Secure Flight Final Rule, and multiple PIA and SORN updates. TSA also publishes information regarding Secure Flight on www.tsa.gov.[26] Lastly, covered aircraft operators are required to provide notice to individuals at the time they make a reservation.

While many of these notices allude to the relationship between CBP and TSA in the pre-screening process, CBP is publishing this PIA update Addendum to ATS to give clearer notice about the types of flights impacted, and specific notice of CBP's use of the SFPD.

Privacy Risk: There is a risk that CBP's use of Secure Flight data does not align with previously published notices and regulations regarding the Secure Flight program, and that the changes will take place without adequate notice and comment from the public.

Mitigation: This use is consistent with TSA authorization for CBP to use the SFPD for border security, counterterrorism, significant health threat (e.g., pandemic), and national security purposes.

Privacy Risk: There is a risk that passengers aboard U.S. and foreign air carriers that fly over the United States (i.e., overflights), but never touch down into the United States, such as flights from Mexico to Canada, and individuals aboard U.S. carriers that fly from one international point to another international point (i.e., point-to-point flights), such as Berlin to Shanghai, will not be aware that their information is being shared with CBP and may impact their future travel to the United States.

Mitigation: This risk is partially mitigated. This PIA provides notice of the sharing of this data within DHS for the purposes outlined above and consistent with restrictions and safeguarding of such data that is required by law and DHS policies.

Data Retention by the project

CBP will retain SFPD in ATS and TECS consistent with the records retention schedules for ATS and TECS, which are consistent with the Secure Flight records retention schedule.

[26] *See* https://www.tsa.gov/travel/security-screening for additional information.

Specifically, ATS will retain: 1) all confirmed watchlist matches for 15 years; 2) all possible but subsequently cleared watchlist matches for 7 years; 3) rule hits for 7 years; and 4) non-matches for 7 days to be able to create, modify, and run rules, as well as to conduct additional analysis on the data. In addition, records created about an individual associated with a confirmed or possible match to a watchlist or rule hit that require additional analysis in the ATS case management module ATS-TF will be retained for 15 (confirmed match) and 7 (possible match and rule hit) years. However, data that is linked to a border security, national security, significant health risk, or counterterrorism matter, will be retained in ATS for the life of the matter to support that activity and other similar activities that may become related.

TSA SFPD Records Retention Schedule

The TSA Secure Flight records schedule retains: 1) confirmed watch list hits for 99 years, 2) possible watch list hits for 7 years, and 3) rules-based hits for 7 years.

TECS Records

CBP may insert records in TECS on individuals who may need additional scrutiny when entering the United States. If a record is inserted in TECS on such an individual, CBP will retain SFPD in TECS consistent with the TSA retention schedule (i.e., 7 years – possible watchlist match; 7 years – rule hits; 7 days – no match; and 75 years – watchlist matches, consistent with the TECS schedule). However, data that is linked to a specific border security, national security, significant health risk, or counterterrorism matter, will be retained in TECS for the life of the matter to support that activity and other similar activities that may become related.

Privacy Risk: There is a privacy risk that CBP will retain information beyond the existing, narrow Secure Flight retention period.

Mitigation: CBP will adhere to the designated retention schedules for SFPD data, which are consistent with the TSA retention schedules. To ensure compliance with these retention schedules, CBP Privacy will conduct a CPE within 6 months of the NTC beginning regular ingest of the SFPD to evaluate these risks and mitigations. The results of the CPE will be shared with the DHS Privacy Office.

Information Sharing

Dissemination of overflight or international to international SFPD is prohibited except as required to perform passenger screening operations or border security operations, except that terrorism and national security information may be shared, as required by law.

Privacy Risk: There is a privacy risk that CBP will share SFPD information outside of DHS without TSA's authorization.

Mitigation: TSA and CBP have worked together on processes and procedures to ensure proper coordination on the sharing of SFPD information outside of DHS. In addition, CBP Privacy

will conduct a CPE within 6 months of the NTC beginning regular ingest of the SFPD to evaluate these risks and mitigations. The results of the CPE will be shared with the DHS Privacy Office.

Redress

Redress methods remain unchanged from the original ATS PIA. Most of the information within ATS is submitted from underlying source datasets. To the extent that a record is exempted in a source system, the exemption will continue to apply. Because of the law enforcement nature of ATS, DHS has exempted portions of this system from the notification, access, amendment, and certain accounting provisions of the Privacy Act. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records with appropriate exemptions in place.

Privacy Risk: Individuals may not receive the level of redress they desire.

Mitigation: This risk is mitigated, to extent possible consistent with law enforcement and national security exemptions noted in the applicable SORNs. DHS has a robust redress process to assist travelers who believe they are subject to improper scrutiny.

A traveler, regardless of his or her citizenship or residence, may obtain access to his or her PNR. However, records concerning the targeting rules, the responses to rules, case events, law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information, information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department, or records exempted from access by the system from which ATS ingested or accessed the information will not be accessible to the individual.

Notwithstanding the applicable exemptions, CBP reviews all such requests on a case-by-case basis. If compliance with a request would not interfere with or adversely affect the national security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of CBP in accordance with procedures and points of contact published in the applicable SORN.

If a traveler believes that CBP actions are the result of incorrect or inaccurate information, then inquiries may be directed to:

CBP INFO Center
OPA—Rosslyn
U.S. Customs and Border Protection
1300 Pennsylvania Avenue
Washington, D.C. 20229

Travelers may also contact DHS TRIP, 601 South 12th Street, TSA-901, Arlington, VA 22202 or online at www.dhs.gov/trip. Individuals making inquiries may be asked to provide additional identifying information to enable DHS to identify the record(s) at issue.

Auditing and Accountability

There are no changes to the auditing and accountability procedures for ATS as described in the previously issued ATS PIAs. ATS has ability to track no matches, possible matches, rule matches, and confirmed matches and will implement purge scripts per the stated retention policy.

ATS PIA Update Addendum 2:

Updated Populations Subject to ATS Vetting

2.1 CBP Trusted Traveler and Trusted Worker Populations

January 13, 2017 *(back to top)*

The Global Enrollment System (GES) allows CBP Officers to facilitate enrollment of and vetting processes for trusted traveler, trusted worker, and registered traveler programs[27] in a centralized environment. It serves as the primary repository for enrollment, application, and background investigation data and supports over six million enrollees. Enrollment in these programs enables CBP to expedite the inspection and security process for lower risk travelers and workers and allows more scrutiny for individuals who present an unknown risk.[28]

Previously, CBP submitted a list of all GES enrollees on a nightly basis to the FBI and the National Crime Information Center (NCIC) replied with a response for every enrollee. This approach:

- Used a large amount of system resources;
- Raised bandwidth issues and delays during normal processing transmissions;
- Prevented real-time responses (24-hour delays on occasions); and
- Increased the privacy and IT security risks associated with transmission of the data.

The NCIC/Nlets Recurrent Vetting Service (NNVS) within the TECS Platform replaces nightly trusted traveler vetting. The new process submits an initial batch containing millions of GES traveler records (with periodic updates for additions/deletions) to the FBI and NCIC responds in real time with information only pertaining to individuals that have experienced an update in their records or vetting results. ATS will enable this recurrent vetting process for trusted travelers, which is already being vetted through the ATS platform during initial submission. This new process:

- Alleviates the need to return the full dataset of trusted traveler records to CBP every evening;
- Provides a real-time response instead of a potential 24-hour delay;
- Uses less processing/transmission resources; and

[27] Trusted travelers and registered traveler programs typically require the same or similar types of PII to be submitted by an individual; the difference between these programs is the level and frequency of vetting conducted on individuals who apply to participate. For example, trusted traveler programs require recurrent vetting of individuals for the full duration of the benefit; while registered travelers do not.

[28] For a detailed description of trusted traveler and trusted worker programs, please see DHS/CBP/PIA-002 Global Enrollment System and subsequent updates, *available at* https://www.dhs.gov/publication/global-enrollment-system-ges.

- Decreases privacy and IT security risks through reduced dataset transmissions and exposure.

No new information is collected as part of this recurrent vetting process. This modification does not alter the PII CBP obtains to perform background checks on trusted travelers or workers or the privacy posture of TECS.[29]

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

All of the authorities previously identified for ATS remain in effect. ATS derives its authority primarily from 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582; 8 U.S.C. § 1357; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347).

All previously identified SORNs remain in effect, or are noted under the "Notice" section below.

Characterization of the Information

Historically, CBP has sent a nightly data extract directly to the FBI/NCIC for the vetting of trusted traveler and trusted worker populations. In the new process, the same information will be provided in bulk via TECS to the NNVS for recurrent vetting; only new or updated records will be resubmitted. These data elements include all biographic elements described in the previously issued GES PIAs, and photographs and fingerprints collected as part of the applicant interview process.[30]

Privacy Risk: There are no new privacy risks regarding characterization of information related to the recurrent vetting of trusted traveler and trusted worker populations. Recurrent vetting relies upon the same information and sources as the previous nightly batch process. In addition,

[29] For a more detailed description of the GES vetting process, please *see* DHS/CBP/PIA-002(c) Global Enrollment System (GES) (November 1, 2016), *available at* https://www.dhs.gov/publication/global-enrollment-system-ges.
[30] As part of the vetting process, CBP also conducts an interview with the applicant and may retain a photograph and fingerprints of the applicant. Photographs and biometrics of trusted travelers are maintained in the DHS Automated Biometric Identification System (IDENT). For more information about the system please *see* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) (December 7, 2012), *available at* https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system.

the elimination of nightly transmission of batch data is privacy protective, reducing the amount of sensitive information in transit thereby reducing the risk of loss or compromise.

However, the previously identified risks in the GES PIA[31] remain. There is a risk that inaccurate data input into GES by either the individual applying for the trusted traveler, registered traveler, or trusted worker program or by the CBP Officer may result in an erroneous decision to approve or disapprove enrollment in a particular program.

Mitigation: CBP mitigates this risk by conducting personal interviews of applicants for trusted traveler and registered traveler, and trusted worker programs. If there are doubts concerning whether the individual applying for the program is the same individual of record in a law enforcement database, or if that database record raised accuracy concerns, CBP may use the personal interview and the application data to verify the information. CBP offers the applicant an opportunity to reapply and clarify the potential inaccuracy.

Uses of the Information

Enrollment in trusted population programs enables CBP to expedite the inspection and security process for lower risk travelers and workers and allows more scrutiny for individuals who present an unknown risk. As described in detail above, the proposed changes to recurrent vetting both increases operational efficiencies for CBP, and closes the security gaps posed by a potential 24-hour delay of relevant information.

Privacy Risk: There are no new risks regarding use of information posed by recurrent vetting of trusted populations. Recurrent vetting limits the amount of information shared outside of CBP for vetting, and decreases the risk of unauthorized access or mishandling.

However, the previously identified risks in the GES PIA remain. There remains a risk that information used to enroll individuals in a trusted traveler, registered traveler, or trusted worker program will be used for a purpose inconsistent with the original collection.

Mitigation: This risk is mitigated by the manner in which CBP collects and stores information for trusted traveler, registered traveler, and trusted worker programs. CBP manages the various programs in separate environments, which can interface when an applicant applies for a separate GES-managed program. The data segregation also supports software management for the various programs. Additionally, all system users are trained to use information strictly for determining program eligibility. Access to GES is granted to users by a limited number of system administrators and access level varies based on a need-to-know and the user's role. Users are also required to take annual privacy training to ensure that they know and understand the importance of managing sensitive PII.

[31] *See* DHS/CBP/PIA-002(c) Global Enrollment System (GES) (November 1, 2016), a*vailable at* https://www.dhs.gov/publication/global-enrollment-system-ges.

Notice

CBP is conducting this PIA update to provide notice of changes to CBP's vetting of trusted traveler and trusted worker populations. In addition to this PIA update, CBP recently published an update to the GES PIA to describe (a) the expansion of CBP's trusted worker program(s) and (b) the recurrent vetting process.

CBP collection of information for trusted traveler vetting purposes is covered by the Global Enrollment System SORN.[32] CBP collection of information for trusted worker populations is covered by the Persons Engaged in International Trade in Customs and Border Protection Licensed/Regulated Activities SORN.[33]

Privacy Risk: There is a risk to notice that applicants and enrollees may not know how CBP may use their information submitted to the GES.

Mitigation: CBP mitigates this risk by publishing a series of GES PIAs and the applicable SORNs, which provide transparency into GES information usage. This PIA also provides notice on how the information submitted to CBP will be recurrently vetted through the ATS platform.

Data Retention by the project

There are no changes to the retention of data for vetting trusted traveler and trusted worker populations. Global enrollment data continues to be retained for the duration of the individual's active membership (in increments of a 5-year term), plus 3 years after the membership is no longer active. There are no new privacy risks related to retention.

Information Sharing

There are no changes to information sharing from previously issued GES PIAs related to trusted traveler and trusted worker vetting.

Redress

For all of the various ATS updates, redress methods remain unchanged from the original ATS PIA. Most of the information within ATS is submitted from underlying source datasets. To the extent that a record is exempted in a source system, the exemption will continue to apply. Because of the law enforcement nature of ATS, DHS has exempted portions of this system from the notification, access, amendment, and certain accounting provisions of the Privacy Act. These exemptions also apply to the extent that information in this system of records is recompiled or is

[32] *See* DHS/CBP-002 Global Enrollment System, 78 FR 3441 (January 16, 2013), *available at* https://www.gpo.gov/fdsys/pkg/FR-2013-01-16/html/2013-00804.htm.
[33] *See* DHS/CBP-010 Persons Engaged in International Trade in Customs and Border Protection Licensed/Regulated Activities, 75 FR 77753 (December 19, 2008), *available at* https://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29799.htm.

created from information contained in other systems of records with appropriate exemptions in place.

There is no privacy risk to redress for this information. CBP provides applicants who are denied acceptance into a trusted traveler, trusted worker, or registered traveler program with a personal letter that provides a clear and concise statement of why it denied the application. Individuals may also file for redress using the access, correction, and amendment process described above.

Auditing and Accountability

There are no changes to the auditing and accountability procedures for ATS as described in the previously issued ATS PIAs.

2.2 Immigration Benefit Applicants and Petitioners

January 13, 2017 *(back to top)*

Visa Application Vetting

ATS-P is currently used to vet non-immigrant and immigrant visa applications for the Department of State (DOS). DOS sends online visa application data to ATS-P for pre-adjudication investigative screening. ATS-P vets the visa application and provides a response to the DOS Consular Consolidated Database (CCD) indicating whether or not derogatory information was identified by DHS about the visa applicant. Applications of individuals for whom derogatory information is identified are referred for manual review to the appropriate agency conducting the vetting. If, following manual review, an applicant is determined to be eligible for a visa, an updated response is sent to CCD. If the manual review does not result in any change to the individual's eligibility, an additional processing occurs in the ICE Visa Security Program Tracking System (VSPTS-Net)[34] case management system, after which updated information (including relevant case notes) regarding eligibility is provided to both CBP and CCD.

Refugee Vetting

Pursuant to various information sharing documents, DHS, DOS, and several vetting agencies in the law enforcement and intelligence community have developed a process to share refugee application data in DOS's Worldwide Refugee Admissions Processing System (WRAPS) to enable vetting of DOS WRAPS data against each agency's respective holdings to identify possible derogatory information related to individuals seeking refugee status. ATS is used as a vehicle to transmit application data to partner agencies in the law enforcement and intelligence community. At present, CBP does not retain refugee application data nor does it conduct independent vetting.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

All of the authorities previously identified for ATS remain in effect. ATS derives its authority primarily from 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582; 8 U.S.C. § 1357; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347). See also, e.g., 6 U.S.C. §§ 111, 211; 8 U.S.C. §§

[34] *See* DHS/ICE/PIA-011(a) Visa Security Program Tracking System (VSPTS-Net) (January 17, 2013), *available at* https://www.dhs.gov/publication/dhsicepia-011-visa-security-program-tracking-system-vspts-net.

1103, 1182, 1225, 1225a, 1324; 19 U.S.C. §§ 1431, 1433, 1436, 1448, 1459, 1590, 1594, 1623, 1624, 1644, 1644a.

USCIS collects, retains, and shares immigration benefit applicant and petitioner data in accordance with a variety of SORNs, including: Alien File, Index, and National File Tracking System of Records;[35] Background Check Service;[36] Inter-Country Adoptions Security;[37] Benefits Information System;[38] Asylum Information and Pre-Screening System of Records;[39] and Refugee Case Processing and Security Screening Information System of Records.[40]

DOS maintains refugee applicant information in accordance with the Refugee Case Records SORN.[41]

All previously identified CBP SORNs remain in effect, or are noted under the "Notice" section below.

Characterization of the Information

DOS provides the applicant's information via DOS WRAPS to USCIS through the Enterprise Service Bus (ESB) and onward for ingestion into the Case and Activity Management for International Operations (CAMINO).[42] USCIS also passes the DOS WRAPS information to ATS. ATS serves as a technical pass through, providing the information to vetting partners which may result in a match to derogatory holdings, when it exists. Any information that is returned by ATS is sent to CAMINO, which is then used by USCIS personnel to compile and provide a final response to DOS WRAPS. The responses are considered by DOS for determination regarding issuance of a visa and by USCIS for its determination on whether to grant the benefit.

ATS only retains audit information related to when CBP receives or transmits the refugee application data. Once the data is sent to the law enforcement and intelligence community, CBP

---

[35] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69983 (November 22, 2013), *available at* https://www.gpo.gov/fdsys/pkg/FR-2013-11-21/html/2013-27895.htm.
[36] *See* DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007), *available at* https://www.gpo.gov/fdsys/pkg/FR-2007-06-05/html/07-2782.htm.
[37] *See* DHS/USCIS-005 Inter-Country Adoptions Security, 81 FR 78614 (November 8, 2016), *available at* https://www.regulations.gov/document?D=DHS-2016-0071-0001.
[38] *See* DHS/USCIS-007 Benefits Information System, 81 FR 72069 (October 19, 2016), *available at* https://www.regulations.gov/document?D=DHS_FRDOC_0001-1511.
[39] *See* DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (November 30, 2015), *available at* https://www.gpo.gov/fdsys/pkg/FR-2015-11-30/html/2015-30270.htm.
[40] *See* DHS/USCIS–017 Refugee Case Processing and Security Screening Information System of Records, 81 FR 72075 (October 19, 2016), *available at* https://www.regulations.gov/document?D=DHS_FRDOC_0001-1512.
[41] *See* State-59, Refugee Case Records, (February 6, 2012), *available at* http://www.state.gov/documents/organization/242608.pdf.
[42] CAMINO is a person-centric case management system used to administer, track, and adjudicate applications filed with or processed by USCIS International Operations (IO) offices under IO jurisdiction with an international nexus. For a full privacy risk analysis of CAMINO, please *see* DHS/USCIS/PIA-051 Case and Activity Management for International Operations (CAMINO) (May 26, 2015), *available at* https://www.dhs.gov/publication/dhs-uscis-pia-051-case-and-activity-management-international-operations-camino.

deletes the refugee application information in ATS except for an audit log, which includes: 1) a request identification number, 2) the date/time the DOS WRAPS data was received from CAMINO, and 3) the date/time responses were received and transmitted from the vetting agencies.

Uses of the Information

The upgraded functionality of ATS allows automation of the refugee process supporting both CBP and USCIS missions of border security and immigration integrity respectively. ATS facilitates the automated vetting of all refugee information against partner holdings. This transactional approach to refugee processing provides expedited and more accurate vetting of refugees, promotes earlier eligibility determinations, and enables recurrent review of refugees.

Notice

CBP is conducting this PIA update to provide notice of the use of ATS in the automation of refugee and other immigration benefit application processing. There are no new privacy risks to notice identified with this initiative. CBP already conducts these checks on a manual basis for USCIS.

Data Retention by the project

CBP is only retaining an audit log of the information sharing. No PII is retained by CBP in this process.

Information Sharing

The automation of refugee vetting using ATS entails automated sharing of information between the DOS, CBP, USCIS, and other vetting agencies. As implemented, refugee information from DOS is matched in an automated manner against vetting partners' holdings. DOS provides the applicant's information to USCIS for ingestion, which is then transmitted to ATS. Vetting agencies' responses are returned through ATS, which then routes the information back to the DOS via USCIS. There is no new privacy risk to information sharing because CBP already conducts these checks on a manual basis for USCIS.

Redress

For all of the various ATS updates, redress methods remain unchanged from the original ATS PIA. Most of the information within ATS is submitted from underlying source datasets. To the extent that a record is exempted in a source system, the exemption will continue to apply. Because of the law enforcement nature of ATS, DHS has exempted portions of this system from the notification, access, amendment, and certain accounting provisions of the Privacy Act. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records with appropriate exemptions in place.

For USCIS data specifically, an individual may gain access to his or her USCIS records by filing a Privacy Act request. If an individual would like to file a Privacy Act request to view his or her USCIS record, he or she may mail the request to the following address:

National Records Center
Freedom of Information Act (FOIA)/Privacy Act Program
P.O. Box 648010
Lee's Summit, MO 64064-8010

USCIS SORNs, including those specified in this PIA, provide specific information about what information may be accessed and how. The information requested may be exempt from disclosure under the Privacy Act because some USCIS systems of record may contain law enforcement sensitive information, the release of which could possibly compromise ongoing criminal investigations. Further information about Privacy Act and FOIA requests for USCIS records is available at http://www.uscis.gov.

Privacy Risk: There is a risk that individuals will not have redress from external partner agencies with which USCIS and CBP share information.

Mitigation: USCIS and CBP have mitigated this risk to the best extent possible. USCIS sends to and obtains information from external agencies. These external agencies are fully responsible for any data that they provide to USCIS. They are responsible for maintaining accurate records obtained from USCIS. The external agencies provide procedures for access and redress in accordance with FOIA and the Privacy Act.

Auditing and Accountability

There are no changes to the auditing and accountability procedures for ATS as described in the previously issued ATS PIAs. All ATS auditing, accountability, and access control features will be applied to the refugee information as well. The Targeting and Analysis Systems Program Directorate will implement purge scripts to comply with the retention requirements. ATS keeps an audit trail of information into/out of/deleted from ATS. User roles to limit access to this data will also be implemented.

2.3 Retention of Information from Electronic Devices in the Automated Targeting System-Targeting Framework

April 28, 2017 *(back to top)*

The Automated Targeting System-Targeting Framework (ATS-TF) is a module within ATS used by a limited number of users to track information of targeting interest regarding travelers and cargo. ATS-TF permits a user to search across the data sources available in the other modules of ATS based on role-based access for research and analysis purposes. ATS-TF provides users with the ability to: 1) initiate research activities, 2) collaborate with other analysts, and 3) use past activity logs as additional information sources by tracking past research activity with respect to persons and entities of interest. ATS-TF allows the creation of long-term projects or operational and analytical reports that may include public source information obtained by users for reference or incorporation into the report or project. Through the ATS-TF web interface, authorized CBP personnel can create ad hoc queries that allow users to find information related to a specific activity or entity contained within each event. ATS-TF allows users to integrate data from multiple sources and show possible relationships between entities and data elements.[43]

Consistent with the CBP directive, *Border Search of Electronic Devices Containing Information*,[44] CBP conducts searches of electronic devices of travelers entering and exiting the United States to ensure compliance with customs, immigration, and other laws enforced by CBP. These searches are part of CBP's long-standing practice and are essential to enforcing the law at the U.S. border and to protecting border security, including to assist in detecting evidence relating to terrorism and other national security matters, narcotics, human and bulk cash smuggling, and export violations, and are often integral to a determination of admissibility under the immigration laws. The actions undertaken during a border search depend on the circumstances. Border searches of electronic devices may include searches of the information physically resident on the device when it is presented for inspection, or during its detention by CBP for an inbound or outbound border inspection. A CBP Officer or Agent may detain electronic devices, or copies of information physically resident on the device,[45] for a brief, reasonable period of time to perform a thorough border search, subject to various requirements in the CBP directive, Border Search of Electronic Devices Containing Information. For example, supervisory approval is required to detain or seize an electronic device or a copy of information contained therein for continuation of a border search after the individual departs the port of entry or other location of detention. The search of the electronic devices will be documented and searches should be conducted in the presence of the

[43] For a complete assessment of the rules process and procedures within ATS, *see* DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update (June 1, 2012), *available at* https://www.dhs.gov/topic/privacy.
[44] *See* Directive No. 3340-049 (August 20, 2009), *available at* https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf.
[45] Information physically resident on the device is available when the device is not connected to the internet or any network.

traveler whose information is being examined unless there are national security, law enforcement, or other operational considerations that make it inappropriate to permit the individual to remain present.

Section 5.4.1.2 of the CBP directive, *Border Search of Electronic Devices Containing Information*, provides for retention of information in CBP Privacy Act-Compliant Systems and states that without probable cause to seize an electronic device or a copy of information contained therein, CBP may retain only information relating to immigration, customs, and/or other enforcement matters if such retention is consistent with the privacy and data protection standards of the system of records in which such information is retained. CBP's collection of information from electronic devices is discussed in detail in other privacy compliance documentation.[46] Searches of electronic devices will be documented.

To further CBP's border security mission, CBP may use ATS to further review, analyze, and assess the information physically resident on the electronic devices, or copies thereof, that CBP collected from individuals who are of significant law enforcement, counterterrorism, or other national security concerns. CBP may retain information from the physical device and the report containing the analytical results, which are relevant to immigration, customs, and/or other enforcement matters, in ATS-TF for purposes of CBP's border security mission, including identifying individuals who and cargo that need additional scrutiny. CBP may use ATS-TF to vet the information collected from the electronic devices of individuals of concern against CBP holdings and create a report which includes data that may be linked to illicit activity or actors. Information from electronic devices uploaded into ATS will be normalized[47] and flagged as originating from an electronic device.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

ATS derives its authority primarily from 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582; 8 U.S.C. § 1357; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347).

[46] *See* DHS/CBP/PIA-008 Border Searches of Electronic Devices (August 25, 2009), *available at* https://www.dhs.gov/topic/privacy.

[47] Normalization is the process of organizing data in a database to reduce redundancy and ensure that related items are stored together.

CBP's authorities to search and retain information obtained from travelers, including from electronic devices, derives from the following: 8 U.S.C. § 1357; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1595a; 31 U.S.C. § 5317; 22 U.S.C. § 401.

CBP retains copies of information from electronic devices and the report containing the analytical results in ATS, only when it relates to customs, immigration, or other enforcement matters, in accordance with the CBP directive, *Border Search of Electronic Devices Containing Information,* and the National Archives and Records Administration (NARA) approved retention schedule as reflected in the Automated Targeting System (ATS) System of Records Notice.[48]

Characterization of the Information

CBP conducts searches of electronic devices at the border, both inbound and outbound, to ensure compliance with customs, immigration, and other laws enforced by CBP. These searches are part of CBP's long-standing practice and are essential to enforcing the law at the U.S. border, and to protecting border security, including to assist in detecting evidence relating to terrorism and other national security matters, narcotics, human and bulk cash smuggling, and export violations, and are often integral to a determination of admissibility under the immigration laws. CBP only copies information from electronic devices and retains that information in ATS relating to customs, immigration, or other enforcement matters, including for example, terrorism or narcotics.

Privacy Risk: There are privacy risks associated with the volume and breadth of information from electronic devices stored in ATS.

Mitigation: This risk is partially mitigated. CBP may use ATS to further review, analyze, and assess electronic information collected from individuals who are of significant law enforcement, counterterrorism, or other national security concerns, consistent with CBP's border security mission. In addition, CBP follows all of the reporting, handling, and other requirements in the CBP Directive, *Border Search of Electronic Devices Containing Information*, including the requirements outlined in the review and handling of privileged or other sensitive material section.

Privacy Risk: There is a risk that information from electronic devices in ATS is inaccurate.

Mitigation: This risk is not mitigated. CBP is obtaining this information directly from the electronic device, but it remains possible that data on the device may not be accurate. CBP will use this information to match against CBP holdings and will take action on information obtained from an electronic device if, based on information available to CBP, the information is assessed to be accurate and reliable. The information will be used to facilitate additional lines of inquiries, to corroborate existing information, and to identify those travelers and cargo that needs additional scrutiny.

Uses of the Information

[48] *See* DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).

ATS may be used to conduct an analytic review of the information and will transfer results of that review to ATS-TF. ATS-TF may retain the analytic review, which includes the information that may be linked to illicit activity or illicit actors and the underlying information relating to immigration, customs, and/or other enforcement matters for the purposes of ensuring compliance with laws CBP is authorized to enforce and to further CBP's border security mission, including identifying individuals who and cargo that need additional scrutiny and other law enforcement, national security, and counterterrorism purposes. For example, CBP may use ATS to link a common phone number to three separate known or suspected narcotics smugglers, which may lead CBP to conduct additional research and, based on all available information, further illuminate a narcotics smuggling operation. Access to this information will be restricted by technical security and user profiles.

Privacy Risk: There are privacy risks associated with use limitation, given the breadth of information collected from electronic devices, some of which may bear no relevance to any law enforcement matter. There are additional risks that ATS may use information collected from electronic devices to link to individuals who were not subjects of the original collection of the information.

Mitigation: This risk is partially mitigated. CBP limits the use of ATS for analysis of electronic information collected from individuals who are of significant law enforcement, counterterrorism, or other national security concerns. To reduce privacy risks associated with the retention of sensitive information, CBP follows all of the reporting, handling, and other requirements in the CBP Directive, *Border Search of Electronic Devices Containing Information*, including the requirements outlined in the review and handling of privileged or other sensitive material section. Some risk remains, however, that information linked to individuals who are not subjects of the original collection may be retained.

Notice

CBP provides a variety of forms of notice to individuals related to searches of possessions, including electronic devices. For example, signage posted at official ports of entry indicate that all belongings are subject to search. In addition, when a border search of information is conducted on an electronic device, and when the fact of conducting this search can be disclosed to the individual transporting the device without hampering national security, law enforcement, or other operational considerations, the individual may be notified of the purpose and authority for these types of searches, how the individual may obtain more information on reporting concerns about the search, and how the individual may seek redress from the agency if he or she feels aggrieved by a search. Despite these various forms of notice, CBP does not provide specific notice at time of collection that this information may be retained in ATS. Accordingly, CBP is conducting this PIA update to provide notice of the use of ATS to analyze and retain information from electronic devices searched at the border, relating to immigration, customs, and/or other enforcement matters for the purposes of ensuring compliance with laws CBP is authorized to enforce.

Privacy Risk: There is a risk that individuals whose information is obtained from electronic devices will not be aware that some of this information may be retained in ATS.

Mitigation: This risk cannot be fully mitigated. However, CBP is publishing this PIA update to provide specific notice that ATS may analyze and retain information collected from electronic devices. Because CBP does not provide specific notice at the time of collection, however, some risk remains. This is a similar risk posed by other law enforcement information collections, since the nature of law enforcement activities and operations does not always enable specific, on-time notice.

Data Retention by the project

The information in ATS will be retained consistent with the established NARA schedule, as reflected in the ATS SORN. The retention period for the official records maintained in ATS will not exceed 15 years, after which time the records will be deleted, except information maintained only in ATS that is "linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases (i.e., specific and credible threats; flights, individuals, and routes of concern; or other defined sets of circumstances) will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related."

Privacy Risk: There is a risk CBP will retain in ATS sensitive information obtained from electronic devices that is unrelated to any law enforcement matter.

Mitigation: This risk is partially mitigated. CBP conducts its activities involving the border search of electronic devices containing information consistent with the CBP Directive, *Border Search of Electronic Devices Containing Information.* Pursuant to the CBP Directive, without probable cause to seize an electronic device or copy of information contained therein, CBP may retain only information relating to immigration, customs, and/or other enforcement matters if such retention is consistent with the privacy and data protection standards of the system of records in which such information is retained. Consistent with the CBP Directive and the ATS SORN, CBP may use ATS to further review, analyze, and assess the copy of the electronic information collected from individuals who are of significant law enforcement, counterterrorism, or other national security concerns. CBP may retain the information from the electronic device and the report containing the analytical results, which are relevant to immigration, customs, and/or other enforcement matters, in ATS for CBP's border security mission, including identifying individuals and cargo needing additional scrutiny.

Information Sharing

Absent any legal prohibitions, CBP may share information from ATS with other DHS Component personnel who have an authorized purpose for accessing the information in performance of their duties, possess the requisite security clearance, and assure adequate

safeguarding and protection of the information. In addition, CBP may share information with external agencies consistent with the routine uses published in the ATS SORN.[49] Specifically, CBP may share information from ATS:

- To appropriate federal, state, tribal, local, or foreign governmental agencies or multilateral government organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where CBP believes the information would assist enforcement of applicable civil or criminal laws (routine use G); and
- To federal or 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 to assist in anti-terrorism efforts (routine use H).

Privacy Risk: There is a risk that CBP will share electronic device information from ATS with outside agencies who do not have a specific need for that information.

Mitigation: CBP mitigates this risk by following the relevant laws and current DHS/CBP policies and procedures associated with the sharing of information and consistent with the routine uses published in the ATS SORN. Any information released would comply with DHS policy and set forth the restrictions on and conditions of use; securing, storing, handling, and safeguarding requirements; and controls on further dissemination.

Redress

For all of the various ATS updates, redress methods remain unchanged from the original ATS PIA. Most of the information within ATS is submitted from underlying source datasets.[50] To the extent that a record is exempted in a source system, the exemption will continue to apply. Because of the law enforcement nature of ATS, DHS has exempted portions of this system from the notification, access, amendment, and certain accounting provisions of the Privacy Act of 1974. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records with appropriate exemptions in place.

Privacy Risk: There is a risk that individuals are not aware of their ability to make record access requests for records in ATS.

Mitigation: This risk is partially mitigated. Previous ATS PIAs and the ATS SORN describe how individuals can make access requests under FOIA or the Privacy Act. In accordance

[49] For a complete list of routine uses, *see* DHS/CBP-006 Automated Targeting System, System of Records, 77 FR 30297 (May 22, 2012).
[50] For more information on ATS data sources, *see* DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update (June 1, 2012), *available at* https://www.dhs.gov/topic/privacy, and DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).

with Executive Order 13768, redress, in the form of seeking access or requesting amendment under the Privacy Act, is now only available for U.S. Citizens, Lawful Permanent Residents (LPR), and persons who are the subject of covered records under the Judicial Redress Act (JRA). For non-U.S. citizens, non-LPRs, and persons not covered by the JRA, access remains available through FOIA. To ensure the accuracy of CBP's records, CBP may accept requests for amendment, regardless of citizenship, on a case-by-case basis, consistent with law.

In addition, providing individual access and/or correction of ATS records may be limited for law enforcement reasons as expressly permitted by the Privacy Act. Permitting access to the records contained in ATS, regardless of a subject's citizenship, 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 the records could also 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. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

Auditing and Accountability

There are no changes to the auditing and accountability procedures for ATS as described in the previously issued ATS PIAs.

The CBP Privacy Office will conduct a CBP Privacy Evaluation (CPE) within one year of publication of this PIA Update. CBP will share the results of the CPE with the DHS Privacy Office.

2.4 Continuous Immigration Vetting

Last updated October 3, 2018 *(back to top)*

Continuous Immigration Vetting

The U.S. Citizenship and Immigration Services (USCIS) Fraud Detection and National Security Directorate (FDNS) is working with the U.S. Custom and Border Protection (CBP) National Targeting Center (NTC) and Targeting and Analysis Systems Program Directorate (TASPD) to enhance and streamline background, identity, and security checks for certain USCIS benefit types through an interagency effort: continuous immigration vetting (CIV).

CIV conducts checks on individuals connected to a USCIS immigration application benefit request against CBP holdings. The process begins with an initial security check upon receipt by USCIS and CBP and continues through the end of the adjudication process. USCIS will use the information provided by CBP to support the adjudication of immigration benefits; specifically, the information will assist in identifying individuals, who may have a connection to potential identity or benefit fraud, national security or public safety concerns, and criminal activity. Trained USCIS personnel review the information returned by CBP and take appropriate actions in accordance with current agency-approved guidelines.

While USCIS already conducts background, identity, and security checks on individuals connected to immigration applications and petitions, CIV enhances the current background check processes by screening and vetting the information against additional CBP holdings. Moreover, CIV would establish recurrent checks against these datasets, which would make benefit processing more efficient.

USCIS is implementing CIV in a phased approach, beginning with automating screening and vetting of immigration applications and petitions, using existing connections among USCIS and CBP supporting other projects. Once fully implemented, ATS will check USCIS immigration application data submitted by USCIS against additional CBP holdings.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

All of the authorities previously identified for ATS remain in effect. ATS derives its authority primarily from 19 U.S.C. §§ 482, 1461, 1496, 1581, and 1582; 8 U.S.C. § 1357; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347). See also 6 U.S.C. §§ 111 and 211; 8 U.S.C.

§§ 1103, 1182, 1225, 1225a, 1324, and 1357; 19 U.S.C. §§ 1431, 1433, 1436, 1448, 1459, 1590, 1594, 1623, 1624, 1644, and 1644a.

USCIS collects, retains, and shares immigration benefit applicant and petitioner data in accordance with a variety of SORNs, including: Alien File, Index, and National File Tracking System of Records;[51] Background Check Service;[52] Inter-Country Adoptions Security;[53] Benefits Information System;[54] and Asylum Information and Pre-Screening System of Records.[55] All previously identified CBP SORNs remain in effect, or are noted under the "Notice" section below.

Characterization of the Information

USCIS and CBP will use ATS to vet applications. The data FDNS sends to CBP will be derived from the applications. This data is outlined in the FDNS PIA (DHS/USCIS/PIA-013-01 Fraud Detection and National Security Directorate (December 16, 2014), available at https://www.dhs.gov/privacy).

In addition to form submission information, USCIS will send to CBP information from the Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT),[56] which may include biographic information, biometric identifier information, and encounter information. ATS is already able to retrieve these data elements through its existing IDENT interface.

ATS will recurrently vet the information against various CBP holdings, including customs, immigration, and terrorism-related information. ATS stops recurrent vetting when it receives a message from USCIS based on administrative closure from an Immigration Judge's calendar or from the Board of Immigration Appeal's docket, certificate of citizenship issue, denial, failure to pay, or withdrawn adjudication activities. In the initial phase of this project, CBP will be required to purge the records upon receipt of notification of an approved status unless that information is linked to active law enforcement lookout records, enforcement activities, or investigations or cases, in which case that data is maintained by CBP in ATS consistent with the ATS retention schedule as reflected in the ATS SORN[57] (*i.e.*, for the life of the law enforcement matter to support that activity and other enforcement activities that may become related). USCIS will also explore expanding these checks to additional benefit types; USCIS and CBP will update compliance documentation as appropriate to account for any expansion.

---

[51] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017).
[52] DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007).
[53] DHS/USCIS-005 Inter-Country Adoptions Security, 81 FR 78614 (November 8, 2016).
[54] DHS/USCIS-007 Benefits Information System, 81 FR 72069 (October 19, 2016).
[55] DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (November 30, 2015).
[56] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* https://www.dhs.gov/privacy.
[57] DHS/CBP-006 Automated Targeting System, System of Records, 77 FR 30297 (May 22, 2012).

Privacy Risk: There is a risk of over-collection of information since CBP may use immigrant application information from USCIS beyond immigration vetting purposes.

Mitigation: This risk is fully mitigated. CBP's mission is to secure the borders while facilitating legitimate trade and travel and includes the enforcement of various immigration laws. CBP's vetting of applications for immigration benefits is pursuant to its agreement with USCIS and in support of the broader mission of DHS. Assisting USCIS benefits the CBP mission by helping identify individuals who need additional scrutiny and ensuring that both agencies have the relevant information needed to carry out their respective duties. CBP will not retain immigration application information upon notice from USCIS of administrative closure from an Immigration Judge's calendar or from the Board of Immigration Appeal's docket, certificate of citizenship issue, denial, failure to pay, or withdrawn adjudication activities, unless that information is linked to active law enforcement lookout records, enforcement activities, or investigations or cases, in which case that data is maintained by CBP in ATS consistent with the ATS retention schedule as reflected in the ATS SORN (*i.e.*, for the life of the law enforcement matter to support that activity and other enforcement activities that may become related).

Uses of the Information

USCIS FDNS and CBP will use ATS to enhance and streamline continuous security checks for additional USCIS benefit/request types. ATS will facilitate the automated matching of all application data against partner holdings. While USCIS already conducts background and security checks on individuals connected to immigration applications and petitions, CIV would enhance the current background check processes by matching against additional CBP holdings. Moreover, CIV would establish continuous matching against these datasets, which would close existing security gaps and make benefit/request processing more efficient.

Privacy Risk: There is a risk that CBP will use information from the applications for purposes beyond determining an individual's eligibility.

Mitigation: This risk is mitigated. CBP will not recurrently vet individuals, and it will not retain their information in ATS, once it receives a message from USCIS based on administrative closure from an Immigration Judge's calendar or from the Board of Immigration Appeal's docket, certificate of citizenship issue, denial, failure to pay, or withdrawn adjudication activities, unless that information is linked to active law enforcement lookout records, enforcement activities, or investigations or cases, in which case that data is maintained by CBP in ATS consistent with the ATS retention schedule as reflected in the ATS SORN (*i.e.*, for the life of the law enforcement matter to support that activity and other enforcement activities that may become related).

Privacy Risk: There is a risk that USCIS may store derogatory information in systems that are not authorized to retain law enforcement information.

Mitigation: This risk is mitigated by the fact that, under this program, information CBP provides to USCIS is immediately referred to FDNS for investigation, and any subsequent

derogatory information is retained in the appropriate systems of record authorized to retain enforcement information.

Notice

CBP is conducting this PIA update to provide notice of the use of ATS in the automation of immigration benefit application processing. CBP already conducts these checks on a manual basis for USCIS. In addition, USCIS is updating the FDNS-DS/ATLAS PIA[58] to provide additional notice of this initiative.

Privacy Risk: There is a risk that applicants will not know that their information is being continuously vetted by CBP.

Mitigation: This risk is partially mitigated in that the results under CIV will be filtered through the existing rules-based referral process outlined in the FDNS-DS/ATLAS PIA. Through the PIA, USCIS has provided notice that the following events trigger rules-based referrals and System Generated Notifications (SGNs): 1) when an individual presents him or herself to the agency (*e.g.*, when USCIS receives an individual's benefit request form or while capturing an individual's 10-fingerprints at an authorized biometric capture site, for those forms that require fingerprint checks); 2) when derogatory information is associated with the individual in one or more DHS systems (*i.e.*, ATS); or 3) when FDNS performs an administrative investigation. This risk is further mitigated in that USCIS is updating Appendix A to the PIA to reflect the automated connection to ATS so that individuals are aware that ATS is a new source added to the existing event-based referral process. USCIS's use of the information remains unchanged from the original PIA.

Data Retention by the Project

ATS will continually vet the information against various CBP holdings, including customs immigration, and terrorism-related information until it receives a message from USCIS based on administrative closure from an Immigration Judge's calendar or from the Board of Immigration Appeal's docket, certificate of citizenship issue, denial, failure to pay, or withdrawn adjudication activities. CBP will only retain this information if it is linked to active law enforcement lookout records, enforcement activities, or investigations or cases, in which case that data is maintained by CBP in ATS consistent with the ATS retention schedule as reflected in the ATS SORN (*i.e.*, for the life of the law enforcement matter to support that activity and other enforcement activities that may become related).

Privacy Risk: There is a risk CBP will retain information about individuals after USCIS has made a benefits determination.

[58] *See* DHS/USCIS/PIA-013(a) Fraud Detection and National Security Data System (FDNS-DS) (May 18, 2016), *available at* https://www.dhs.gov/privacy.

Mitigation: This risk is mitigated. ATS will delete the information upon receipt of notification of an approved status unless that information is linked to active law enforcement lookout records, enforcement activities, or investigations or cases, in which case that data is maintained by CBP in ATS consistent with the ATS retention schedule as reflected in the ATS SORN (*i.e.*, for the life of the law enforcement matter to support that activity and other enforcement activities that may become related).

Information Sharing

CBP is collaborating with USCIS to vet information on individuals seeking immigration benefits using ATS. Except as mentioned in this PIA or in other privacy compliance documentation, for external agencies requesting access to USCIS information maintained in ATS, CBP will either refer the requestor to USCIS or seek USCIS's authorization to release the information. Outside of this, there are no changes to information sharing from previously issued ATS PIAs.

Redress

For all of the various ATS updates, redress methods remain unchanged from the original ATS PIA. Most of the information within ATS is submitted from underlying source datasets.[59] To the extent that a record is exempted in a source system, the exemption will continue to apply. Because of the law enforcement nature of ATS, DHS has exempted portions of this system from the notification, access, amendment, and certain accounting provisions of the Privacy Act of 1974. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records with appropriate exemptions in place.

For USCIS data specifically, an individual may gain access to his or her USCIS records by filing a Privacy Act or Freedom of Information Act (FOIA) request. If an individual would like to file a Privacy Act request to view his or her USCIS record, he or she may mail the request to the following address:

National Records Center
Freedom of Information Act (FOIA)/Privacy Act Program
P. O. Box 648010
Lee's Summit, MO 64064-8010

USCIS Systems of Record Notices, including those specified in this PIA, provide specific information about what information may be accessed and how.[60] The information requested may be exempt from disclosure under the Privacy Act because some USCIS systems of record may

[59] DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).
[60] DHS/USCIS-017 Refugee Case Processing and Security Screening Information System of Records, 81 FR 72075 (October 19, 2016).

contain investigatory materials compiled for law enforcement purposes, the release of which could possibly compromise ongoing criminal investigations.[61] Further information about Privacy Act and FOIA requests for USCIS records is available at http://www.uscis.gov.

Privacy Risk: There is a risk that individuals will not have redress from external partner agencies with which USCIS and CBP share information.

Mitigation: USCIS and CBP have mitigated this risk to the fullest extent possible. USCIS sends to and obtains information from external agencies as described in the FDNS Fraud Detection and National Security Data System PIA. These external agencies are fully responsible for any data that they provide to USCIS. They are responsible for maintaining accurate records obtained from USCIS. The external agencies provide procedures for access and redress in accordance with FOIA and Privacy Act.

Auditing and Accountability

ATS auditing capabilities include: automated purge scripts to expunge records that have reached their retention limits; audit trails of information that has been entered into, sent from, and deleted from the system; and user roles that limit access to ATS data. These auditing tools will apply to all USCIS data sets in ATS and will facilitate compliance with the retention and access limitations described in this PIA.

[61] DHS/USCIS-006 Fraud Detection and National Security Records (FDNS) System of Records Notice, 77 FR 47411 (August 8, 2012).

2.5 FinCEN Bank Secrecy Act Data

Last updated October 3, 2018 (back to top)

Overview

U.S. Customs and Border Protection (CBP) and the U.S. Department of Treasury, Financial Crimes Enforcement Network (FinCEN) regularly exchange information in support of both agencies' missions. To further enhance those missions, CBP now ingests Bank Secrecy Act (BSA) data from FinCEN into the Automated Targeting System (ATS). CBP is publishing this Privacy Impact Assessment (PIA) appendix in accordance with the ATS System of Records Notice (SORN), which requires a PIA update to document the ingestion of new data into ATS.

CBP Use of FinCEN Data

FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities. The CBP mission includes the border enforcement of the customs, immigration, and agriculture laws of the United States and the enforcement of hundreds of laws on behalf of numerous federal agencies. FinCEN and CBP have long exchanged data to enhance the missions of both agencies, including enabling CBP to facilitate the investigation of financial crimes with a nexus to the border. While CBP already maintains Currency and Monetary Instrument Reports (CMIRs), CBP began ingesting a broader subset of BSA data into ATS in 2017. BSA data will be available to authorized users via ATS and in the Analytical Framework for Intelligence (AFI).[62] CBP may insert BSA data from ATS into TECS[63] on a case by case basis.

CBP uses BSA data for traveler, cargo, and conveyance analysis and risk assessments in order to identify individuals or entities needing additional scrutiny, including when there is a potential nexus to illicit financing and terrorism related activities. CBP uses BSA data in ATS in order to: (1) make connections among data in CBP holdings related to border security; (2) identify entities, or persons who may need additional scrutiny due to a possible nexus between money, drugs, weapons, and terrorism-related activities; and (3) enhance information available to CBP on known subjects of interest. CBP may also use FinCEN BSA data in support of the ATS risk assessment processes significantly enhancing CBP's advance targeting capabilities.

For example, CBP may use FinCEN data in various algorithms to resolve entities, detect anomalies, or predict patterns based on historical data. In addition, accessing FinCEN data allows authorized ATS users to search data against CBP holdings in ATS or AFI, providing a more comprehensive overview of the person or entity for additional research, analysis, targeting, and/or examination when attempting to cross the border. CBP refreshes the FinCEN data on a daily basis

[62] *See* DHS/CBP/PIA-010 Analytical Framework for Intelligence, *available at* www.dhs.gov/privacy.
[63] *See* DHS/CBP/PIA-TECS System: Primary and Secondary Processing, *available at* www.dhs.gov/privacy.

and tags the source data appropriately within ATS and AFI for auditing purposes.

Restrictions

The following restrictions apply to BSA data from FinCEN ingested into ATS:

- The FinCEN data stored in ATS and access to the data will be maintained in accordance with existing authorization and access control mechanisms in ATS.
- Only authorized users who have been approved by supervisors as having a need to know such information will be allowed to access the FinCEN data. Such access will primarily be for those individuals performing intelligence, analytics, risk assessment, and enforcement functions.
- All requests made to access FinCEN data will be logged, consistent with the existing audit mechanisms available in ATS.
- CBP is required to obtain FinCEN approval before transferring any BSA information from FinCEN to any other information systems.
- Authorized CBP users may only use BSA information from FinCEN on behalf of CBP, consistent with CBP's legal authority, and solely for the purposes of identification, investigation, or prosecution of possible or actual violations of criminal law that fall within the authority of CBP, including related proceedings such as criminal or civil forfeiture proceedings. This includes using BSA information in conjunction with other data sets for traveler, cargo, and conveyance analysis and risk assessments to identify individuals or entities needing additional scrutiny, including when there is a potential nexus to illicit financing and terrorism related activities.

Privacy Impact Analysis

Authorities and Other Requirements

ATS derives its authority primarily from 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582; 8 U.S.C. § 1357; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347).

FinCEN maintains ownership of the data but is permitting CBP to ingest copies of the BSA data into ATS. FinCEN SORN coverage for BSA data is provided by Treasury/FinCEN .003 – Bank Secrecy Act Reports System,[64] which permits sharing with government agencies charged with investigations and administration of law enforcement. FinCEN maintains suspicious activity

[64] 79 F.R. 20974 (April 14, 2014)

reports (SARs) in accordance with the Treasury/FinCEN .002 - Suspicious Activity Report System SORN.[65]

For information of law enforcement interest to CBP, CBP SORN coverage is provided by:

- DHS/CBP-006 Automated Targeting System, which allows ATS to ingest data obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department;[66]
- DHS/CBP-017 Analytical Framework for Intelligence, which allows for AFI ingest of data from the Automated Targeting System (ATS) and other source systems;[67]
- DHS/CBP-011 TECS, which covers the retention of records related to violators or suspected violators of laws enforced or administered by DHS, and information from federal sources pertaining to known or suspected violators;[68] and
- DHS/CBP-024 Intelligence Records System (CIRS), which contains information collected by CBP to support CBP's law enforcement intelligence mission.[69]

Characterization of the Information

ATS may ingest any other information identified by FinCEN and provided pursuant to its authority under 31 U.S.C. § 310.

CBP already maintains Currency and Monetary Instrument Report (CMIR) data in TECS and copies of key elements of TECS data, including CMIR data, are maintained in ATS.

Privacy Risk: There is a risk of overcollection due to the volume of personally identifiable data maintained in FinCEN BSA reports.

Mitigation: This risk is partially mitigated. The BSA requires depository institutions and other industries vulnerable to money laundering to take a number of precautions against financial crime. This includes filing and reporting certain data about financial transactions possibly indicative of money laundering, including cash transactions over $10,000 and suspicious transactions. While the mere filing of these reports has significant value in deterring money laundering, for these reports to be of value in detecting money laundering and other crimes, including those related to terrorism, they must be accessible to law enforcement, counter-terrorism agencies, financial regulators, and the intelligence community. CBP has authority to receive BSA data for purposes of assisting FinCEN and to enhance CBP's border security mission. While CBP

[65] 79 F.R. 20972 (April 14, 2014)
[66] DHS/CBP-006 Automated Targeting System (May 22, 2012) 77 F.R. 30297.
[67] DHS/CBP-017 Analytical Framework for Intelligence System (June 7, 2012) 77 F.R. 13813.
[68] DHS/CBP-011 U.S. Customs and Border Protection TECS (December 19, 2008) 73 F.R. 77778.
[69] DHS/CBP-024 Intelligence Records System (CIRS) System of Records (September 21, 2017) 82 F.R. 44198.

may collect information through BSA reports that does not become part of an investigation or law enforcement activity, CBP attempts to reduce the impacts of this collection by ensuring the data is deleted consistent with ATS retention schedules.

Uses of the Information

CBP uses the BSA data contained in or accessed by ATS in order to: (1) make connections among data in CBP holdings related to border security; (2) identify entities, or persons who may need additional scrutiny due to a possible nexus between money, drugs, weapons, and terrorism related activities; and (3) to enhance information available to CBP on known subjects of interest. The ingestion of FinCEN BSA data for use with ATS risk assessment processes, significantly enhancing CBP's advance targeting capabilities.

For example, CBP uses FinCEN BSA data in various algorithms to resolve entities and detect anomalies or predict patterns based on historical data. In addition, FinCEN BSA data allows authorized ATS users to search data against CBP holdings in ATS, providing a more comprehensive overview of the person or entity for additional research, analysis, targeting, and/or examination when attempting to cross the border.

Privacy Risk: There is a risk that CBP will use BSA data for purposes other than those described in this PIA.

Mitigation: Only authorized users who have been approved by supervisors as having a need to know such information will be allowed to access the BSA data. Such access will primarily be for those individuals performing intelligence, analytics, risk assessment, and enforcement functions. In addition, there is training that will be required for authorized users who access BSA data.

Notice

CBP provides notice to the public of the ingestion of FinCEN BSA data through this PIA. In addition, the FinCEN BSA SORN provides notice of FinCEN's sharing of BSA data with other federal agencies for law enforcement purposes.

Privacy Risk: There is a risk that individuals will be unaware that FinCEN is sharing their data with CBP.

Mitigation: This risk is partially mitigated. CBP provides notice to the public of the ingestion of FinCEN BSA data through this PIA. In addition, the FinCEN BSA SORN provides notice of FinCEN's sharing of BSA data with other federal agencies for law enforcement purposes. However, CBP and FinCEN cannot provide specific notice to individuals that their information is exchanged pursuant to these processes, since this notice may be acknowledgement of, and may interfere with, a criminal investigation.

Data Retention by the project

BSA data will be retained in ATS, AFI, and TECS in accordance with the retention schedules as reflected in the applicable SORNs:

ATS: CBP maintains records in ATS consistent with the retention schedule of the relevant source system, or for no later than fifteen years, unless the record is linked to an active law enforcement lookout record, CBP matches to enforcement activities, or investigations, in which case it will remain accessible for the life of the law enforcement matter in support of that activity and other related enforcement activities.

AFI: Data that has not been incorporated into a finished intelligence product, response to a request for information, or project will follow the source system retention schedule. Projects containing PII may be retained for 30 years and responses to requests for information (RFIs) are retained for 10 years. Finished intelligence products may be retained permanently and transferred to NARA after 20 years.

TECS: CBP retains records in TECS for 75 years or for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

CBP Intelligence Records System (CIRS): To the extent that CBP accesses and incorporates information from other DHS systems of records as sources of information for finished intelligence products, CBP will abide by the safeguards, retention schedules, and dissemination requirements of the underlying source systems of record. CBP retains information consistent with DHS records schedule N1-563-07-016.[70]

Privacy Risk: There are risks associated with the fact that CBP will retain BSA data for different periods of time, depending upon the system into which BSA data is incorporated.

Mitigation: This risk is mitigated. BSA data that does not become associated with another law enforcement or intelligence activity will be retained in ATS for no longer than 15 years, after which point it will be deleted. BSA data from ATS will only be associated with a record in AFI or TECS if it becomes linked to a law enforcement activity, investigation, or intelligence report, in which case the longer retention is appropriate and consistent with the receiving system's purpose and use.

Information Sharing

(FOUO/LES) Pursuant to the Memorandum of Understanding between CBP and FinCEN, CBP may not disseminate BSA information to any person outside CBP, except consistent with the provisions of the FinCEN re-dissemination guidelines which sets forth conditions, restrictions, and reporting requirements for BSA Information. This restriction also applies to case-related information, and to statistical or other information, referencing or revealing BSA information.

[70] DHS/CBP-024 Intelligence Records System (CIRS) System of Records (September 21, 2017) 82 F.R. 44198.

FinCEN may request from CBP reports containing a variety of information, including information related to any dissemination of BSA information.

Redress

FinCEN maintains control of all BSA records in CBP's custody for the purposes of (i) the Freedom of Information Act (FOIA), 5 U.S.C. § 552; (ii) the Privacy Act, 5 USC § 552a; and (iii) any other laws, regulations and policies applicable to the sources, use, disclosure, or dissemination of BSA information in the custody of CBP. CBP must notify FinCEN's Office of Chief Counsel in the event it is served with a subpoena or other request for BSA information as soon as practicable before responding.

For all of the various ATS updates, redress methods remain unchanged from the original ATS PIA. Most of the information within ATS is submitted from underlying source datasets.[71] To the extent that a record is exempted in a source system, the exemption will continue to apply. Because of the law enforcement nature of ATS, DHS has exempted portions of this system from the notification, access, amendment, and certain accounting provisions of the Privacy Act of 1974. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records with appropriate exemptions in place.

Auditing and Accountability

FinCEN intends to train CBP personnel who are authorized to access BSA information on the appropriate handling and safeguarding of BSA data. All CBP personnel accessing BSA information are required to have undergone a satisfactory background investigation and are not eligible to access BSA information until they have completed the required training. CBP intends to notify FinCEN when it revokes an employee's access to BSA data, and will notify FinCEN if it discovers any unauthorized use of or access to the information. CBP will maintain an audit trail of the user, time, and nature of each query of BSA data; CBP may make this audit trail available to FinCEN upon request. FinCEN may also conduct onsite or electronic inspections of CBP's retrieval of BSA information ingested into ATS or accessed via AFI. CBP will refresh the FinCEN data on a daily basis and will tag the source data appropriately within ATS and AFI for auditing purposes. FinCEN may determine that CBP personnel must enter into individual user agreements acknowledging the terms and conditions under which they can obtain access to BSA information from FinCEN.

[71] DHS/CBP-006 Automated Targeting System, 77 Fed. Reg. 30297 (May 22, 2012).

2.6 U.S. Visa Validation Initiative

Last updated December 17, 2018 *(back to top)*

Overview

U.S. Customs and Border Protection (CBP) and the U.S. Department of State (DOS) are working with participating foreign countries to develop a process to use information available through the Automated Targeting System (ATS) to validate U.S. visas presented by third country nationals seeking entry into that foreign country. Several foreign countries exempt certain nationals who seek to enter that foreign country from their standard requirement to obtain a visa from the foreign government if the individual presents a valid and unexpired U.S. visa. As such, the U.S. Government has an agreement and/or arrangement in place with each participating foreign country and developed a process to affirm whether a U.S. visa presented for entry into the foreign country is valid. Specifically, the relevant border security agency of a participating foreign country intends to collect information using the machine readable zone (MRZ) of the U.S. visa presented by a third country national for purposes of applying for admission to the foreign country. The foreign agency will transmit the U.S. visa information to ATS to compare the data provided by the foreign agency against visa information accessed through ATS and provide an automated response to the foreign agency to affirm whether the visa presented is consistent with what is on record. The foreign agency retains responsibility for making all decisions regarding the traveler's admissibility for entry into the foreign country.

CBP seeks to enhance foreign countries' abilities to readily identify individuals who seek to circumvent visa requirements; facilitate the processing of legitimate international travelers; obtain valuable information on the potential attempted use of expired or otherwise invalid U.S. visas; and obtain and provide information that may assist in efforts to protect both countries' borders. This information may also assist the foreign agency and CBP in identifying possible illicit activities including smuggling operations and schemes involving fraudulent documents.

As part of the visa validation program, participating countries will permit CBP to retain the U.S. visa information received from the foreign country, date, port name/port ID, the automated response, and certain information regarding the reason a visa may be invalid. CBP will retain this information consistent with the established National Archives and Records Administration (NARA) schedule, as reflected in the ATS System of Records Notice (SORN). The retention period for the official records maintained in ATS is not to exceed 15 years, after which time the records are to be deleted. However, if the information maintained in ATS becomes "linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases (*i.e.*, specific and credible threats; flights, individuals, and routes of concern; or other defined sets of circumstances)," it is to remain accessible for the life of the law enforcement matter, or 15 years, whichever is longer, to support that activity and other enforcement activities that may become related.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

ATS derives its authority from a variety of laws, such as 19 U.S.C. §§ 482, 1461, 1496, 1581, and 1582; 8 U.S.C. § 1357; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347).

In addition, this initiative is consistent with 6 U.S.C. § 211, 8 U.S.C. § 1202, and 19 U.S.C. § 1628.

The exchange of information under these initiatives is governed by various information sharing agreements in place between the United States Government (CBP and DOS) and the participating foreign country.

CBP retains information in ATS in accordance with the NARA-approved retention schedule as reflected in the ATS SORN.[72]

Characterization of the Information

Border security agencies of participating foreign countries will scan the MRZ of a U.S. visa presented by a traveler seeking entry and send the information to ATS for a validation response. The MRZ of the visa includes the following data elements:

- Name;
- Date of birth;
- Visa number;
- Visa class;
- Passport number;
- Passport issuing country; and
- Gender

CBP will use ATS to compare the data provided by the foreign country against visa information accessed through ATS (through the DOS's Consolidated Consular Database (CCD)) and provide an automated response to the relevant foreign agency indicating whether the visa data

[72] *See* DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).

provided is consistent with information in CCD and if not, certain information regarding the reason a visa may be invalid may also be provided.

ATS will retain records associated with each query containing the data elements submitted by the foreign agency as well as the automated response and certain information regarding the reason a visa may be invalid.

Privacy Risk: There is a risk that CBP may share more information with participating foreign countries than is required for the purposes of visa validation.

Mitigation: This risk is partially mitigated. Under this initiative, CBP is sharing an automated response from ATS specific to the status of the presented U.S. visa, which may include certain information regarding the reason a visa may be invalid and not sharing any other information through the automated process. However, as permitted by applicable law, policy, and with the authorization of the owning agency, CBP may elect to share additional information on a case-by-case basis (for example, if CBP believes the person is of significant law enforcement concern). As a practice, CBP makes note of such sharing in the administrative record associated with the exchange and response maintained in ATS.

Uses of the Information

CBP intends to use the ATS system to compare the data provided by the participating foreign country against visa information accessed through ATS and provide an automated response whether the visa is valid or not. CBP and participating foreign countries use this information to facilitate the flow of legitimate travel while also improving the border security of both countries. The initiative assists CBP's law enforcement mission by preventing the flow of third country nationals who seek to illicitly travel to the United States via foreign countries using fraudulent U.S. documents. In addition, information may also assist the foreign countries and CBP in identifying possible illicit activities including smuggling operations and schemes involving fraudulent feeder documents.

Privacy Risk: There is a risk that U.S. visa data to facilitate the individual's entry into the foreign country is beyond the scope and purpose of the original collection.

Mitigation: This risk is partially mitigated. The issuance of a U.S. visa is for travel to the United States and not to any third countries. While admissibility into foreign countries is outside the original scope of the U.S. visa issuance process, foreign countries may permit U.S. visa holders to use the U.S. visa for entry into their own country. This determination is based on the individual foreign country's legal framework and migration laws, and the ultimate admissibility decision is solely up to the foreign country. If a foreign country opts to recognize a U.S. visa as an acceptable travel document for third country nationals, the U.S. Government may enter into an agreement to conduct visa validation. There is no requirement for travelers to obtain a U.S. visa solely to visit foreign countries, therefore all travelers may continue to apply for a visa to enter that foreign country.

Privacy Risk: There is a risk that the participating foreign country is making an admissibility decision solely based on CBP's response.

Mitigation: This risk is partially mitigated. CBP only provides information about the validity of the U.S. visa. CBP is not providing a determination of admissibility or inadmissibility. The foreign country's migration agency makes the final determination.

Notice

The foreign country provides information to the public regarding the ability of a valid U.S. visa to serve as an exemption to the requirement for obtaining a visa from the foreign country. In addition, CBP is issuing this Privacy Impact Assessment (PIA) to the public to provide additional information about the visa validation initiative.

Privacy Risk: There is a risk that individuals who provide their U.S. visa to a foreign country have no notice their information is being shared with the United States.

Mitigation: This risk is partially mitigated. CBP is issuing this PIA to provide notice to third country nationals, and the foreign countries may provide information to the public about potentially using a U.S. visa to enter the foreign country.

Data Retention by the Project

As noted above, CBP intends to retain the U.S. visa information received from the foreign agency country, date, port name/port ID, as well as a record of the ATS automated response and certain information regarding the reason a visa may be invalid, for 15 years. However, if the record is linked to active law enforcement lookout records, CBP matches to enforcement activities, or investigations or cases, then the record is retained for the life of the law enforcement matter to support that activity and other enforcement activities that may become related, or 15 years, whichever is longer. There are no other changes to the data retention procedures for ATS as described in the previously issued ATS PIAs.

Information Sharing

In general, information in ATS obtained from the foreign agencies may be used or disclosed for purposes of the initiative, including assisting in the effective administration and enforcement of immigration laws and furthering the prevention, detection, or investigation of acts that would constitute a crime. Otherwise, use or disclosure of information provided by any of the foreign agencies is subject to the prior written approval of that foreign agency.

Privacy Risk: There is a risk that the foreign agency will inappropriately share visa data provided by CBP.

Mitigation: This risk is mitigated because CBP through ATS is only sharing non-sensitive automated responses that may include certain information regarding the reason a visa may be invalid. As part of the automated process, CBP/ATS is not sharing any other specific details related

to the traveler, the traveler's immigration status, his or her border crossing history, or any law enforcement information. However, as permitted by applicable law, policy, and with the authorization of the owning agency, CBP may elect to share additional information on a case-by-case basis.

Redress

For all of the various ATS updates, redress methods remain unchanged from the original ATS PIA. Most of the information within ATS is submitted from underlying source datasets.[73] To the extent that a record is exempted in a source system, the exemption will continue to apply. Due to the law enforcement nature of ATS, DHS has exempted portions of this system from the notification, access, amendment, and certain accounting provisions of the Privacy Act of 1974. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records with appropriate exemptions in place.

Privacy Risk: There is a risk that an individual may be denied entry to a foreign country based on information provided by CBP, but will not know to request redress from CBP.

Mitigation: This risk is not mitigated. Individuals are not informed whether the foreign agency's decision regarding admissibility of an individual into its country is based on information provided under this initiative. In addition, foreign countries may decide not to notify the public about this initiative, so an individual may not know to come to CBP for a redress request. However, although the individual may never know to approach CBP for redress, he or she will likely know to reach out to the DOS if the traveler has reason to believe there was an issue with his or her U.S. visa. Any inaccurate information would be corrected by DOS and later updated in ATS, which continuously ingests U.S. visa data.

Auditing and Accountability

The U.S. Government has an agreement and/or arrangement in place with each foreign country participating in this initiative that requires the secure handling and protection of the information, the correction of inaccurate information, and that the information is held in confidence and only used for appropriate purposes. As noted above and under the agreement/arrangement, CBP via ATS is only sharing non-sensitive automated responses that may include certain information regarding the reason a visa may be invalid but is not sharing any other specific details related to the traveler, the traveler's immigration status, his or her border crossing history, or any law enforcement information.

[73] *See* DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).

2.7 Commercial License Plate Reader Information

Last updated July 24, 2019 *(back to top)*

CBP plans to use the Automated Targeting System (ATS) to access commercially available License Plate Reader (LPR) information from a vendor service in order to provide CBP law enforcement personnel with a broader ability to search license plates of interest nationwide. Because license plate readers constitute privacy sensitive technology and LPR information can be combined with other data to identify individuals, CBP is conducting this Privacy Impact Assessment (PIA) addendum to describe how it intends to use the commercial LPR service and explain the measures that will be in place to mitigate concerns regarding the potential impact on the privacy of the public as a result of the use of information obtained from LPR technology.

A number of commercial services collect and aggregate LPR data from both private and public sources and make it available on a fee-for-service basis. Typically, LPR vendors collect license plate image information from private businesses (e.g., parking garages), local governments (e.g., toll booth cameras), law enforcement agencies, and financial institutions via their contracted repossession companies. The LPR commercial aggregator services store, index, and sell access to the images and time and location of collection.

CBP has identified a number of benefits from the use of commercially aggregated LPR data for its law enforcement and border security mission. The data can: 1) identify individuals and vehicles that may need additional scrutiny when attempting to cross the border; 2) enhance both officer and public safety by enabling enforcement actions to occur in locations that minimize the inherent dangers associated with border enforcement encounters; and 3) help resolve matters that might otherwise be closed for lack of viable leads.

In support of these missions, CBP has acquired access to LPR data via an Application Programing Interface (API) to query data aggregated and made available to CBP users by a commercial LPR vendor. CBP accesses the commercial LPR database through the contract provider providing on-demand federated queries through ATS. ATS will not ingest the data; instead, similar to the other existing commercial data interfaces (such as LexisNexis), CBP will create a web service through which authorized ATS users may create vehicle displays that present vehicles of possible interest, query historical LPR data, and use advanced analytics for enhanced review and analysis.

Results of queries via the API are stored in ATS, as well as other CBP systems, such as TECS,[74] Intelligence Reporting System Next Generation (IRS-NG), and Analytical Framework for Intelligence (AFI), if the information is determined to be useful in connection with a legitimate law enforcement or border security mission. This retention will be consistent with the National

[74] LPR data may identify individuals that need additional scrutiny at the border, in which case the LPR information will be used in TECS to create a lookout record.

Archives and Records Administration (NARA) retention schedule as specified in the relevant System of Records Notice[75] (SORN).

Location-based commercially aggregated data creates a number of privacy risks. CBP has taken steps to mitigate these concerns by ensuring that access to this sensitive information is strictly limited and auditable, and by ensuring that all uses of commercially available LPR information are consistent with CBP law enforcement and border security authorities. CBP has limited access to the commercial LPR information through a newly created role within ATS that requires a multi-level approval process. CBP will routinely audit queries of the commercial service to ensure queries are only associated with ongoing enforcement or border security activities. CBP users will utilize LPR data as a tool to further heightened suspicion and generate leads predicated on a relevant CBP mission.

CBP users are permitted to query commercially available LPR information to identify locations and movements of *already identified* subjects and associates believed to be involved in illegal activity in connection with CBP's law enforcement or border security mission. CBP may also use this data to track vehicles suspected of carrying contraband, such as smuggled goods. Users may also use LPR information in conjunction with other law enforcement and/or targeting information to develop leads to further the enforcement matter, including identifying associates of possible concern and eliminating other individuals from further consideration. In addition, CBP may use this information to identify individuals or vehicles which may need additional scrutiny when crossing the border.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

CBP authority to search and maintain commercially available LPR information includes, but is not limited to, 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582; 8 U.S.C. § 1357; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347).

[75] See DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012); DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008); DHS/CBP-017 Analytical Framework for Intelligence, FR 13813 (June 7, 2012).

CBP maintains LPR information in support of its of law enforcement and border security mission under the DHS/CBP-006 Automated Targeting System SORN.[76] As reflected in the SORN, commercial data aggregators are a record source category and used for the purpose of law enforcement and/or research information regarding an individual.

LPR records in support of CBP's law enforcement and border security mission to record information on individuals to whom CBP has issued detentions and warnings are covered under the DHS/CBP-011 TECS SORN.[77]

LPR records collected by CBP to support CBP's law enforcement and border security mission are covered under the System of Records Notice, DHS/CBP-024 CBP Intelligence Records System.[78] This SORN notified the public that data is obtained from commercial data providers, among other sources, in the course of intelligence research, analysis, and reporting.

Characterization of the Information

An LPR is a system consisting of one or more high-speed cameras and related equipment, mounted on vehicles or in fixed locations that automatically and without direct human control locate, focus on and photograph license plates and vehicles that come into range of the device. The system then automatically converts the digital photographic images of license plates and associated data into a computer-readable format. This computer-readable format (also known as "a read") contains some or all of the following information: (1) license plate number; (2) digital image of the license plate as well as the vehicle's make and model; (3) state of registration; (4) camera identification (i.e., camera owner and type); (5) Global Positioning System (GPS) coordinates or other location information taken at the time the information was captured; and (6) date and time of observation. Some LPR systems also capture (within the image) the environment surrounding a vehicle, which may include drivers and passengers. The system seeks to collect information from all vehicles that pass the camera. There is no biographic information about a vehicle owner contained in a license plate capture. However, using data from the commercial LPR database, CBP may conduct additional research and link the license plate data to the VIN and the registered vehicle's information, which may then be linked to suspected vehicles in ATS and/or TECS.

The commercial provider collects LPR data from private and public contributors including law enforcement agencies, local governments, and financial institutions via their contracted repossession companies. CBP will only use LPR data to identify locations and movements of targets and associates believed to be involved in illegal activity in connection with law enforcement or border security mission. For example, LPR data is particularly useful in

[76] *See* DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).
[77] *See* DHS/CBP-011 TECS, 73 FR 7778 (December 19, 2008).
[78] *See* DHS/CBP-024 CBP Intelligence Records System, 82 FR 44198 (September 21, 2017).

enforcement matters in which CBP is attempting to identify or locate members of criminal organizations abetting the movement of terrorists, weapons, narcotics, or smuggled aliens. It is also useful in the detection and identification of tactics, trends, and patterns used by those organizations engaging in illicit activity at the border or attempting to harm the country. Users query the commercial LPR database using a license plate number, address of reader, or make or model of a vehicle the user wants to locate within ATS. The database returns any responsive records, which may include any or all of the above data elements. The search results will contain all LPR reads from the vendor, with a primary focus on reads occurring within the last 30 days. The search results will be maintained temporarily in the cache. Caching of data eliminates the need to repeat the same queries over a short period of time frame. Query results are typically cached for a minimum of four hours, but not more than twenty-four hours, after which they are automatically deleted from the system.

CBP users will create "events" in the ATS-Targeting Framework (TF) to store relevant LPR query responses. ATS-Targeting Framework "events" show what open research projects belong to each user. CBP users will determine whether the query responses are relevant to their research, and if so, may save the query results to the relevant "event." No query responses will be automatically saved. If an LPR result is not relevant to law enforcement or border security missions, users may not save the query result to an event with ATS-TF. All query results that are not uploaded to "events" are automatically deleted from the cache within twenty-four hours. Query responses that are stored in ATS-TF "events" contain only information that is relevant, such as license plate number of a vehicle and the location of a vehicle. CBP users are required to review and validate each item on a "display list" at least once yearly; however, users will be required to update "display lists" as needed when matters are resolved or when the location of a vehicle is no longer of value to law enforcement or border security mission. As stated below, CBP management or oversight personnel will review displays on a quarterly basis and verify those LPR reads that are still relevant to CBP's law enforcement or border security mission.

CBP users will also be able to query LPR data through the AFI search functionality. If the query results are relevant to CBP's law enforcement or border security mission, the results will be added to an AFI Project. An AFI Project will allow CBP users to expand their research, while adding additional data sources to compile connections between a vehicle and an address know for criminal activity. This information may help CBP to identify individuals, or vehicles, involved in criminal activity who may need additional scrutiny when attempting to cross the border or to identify and locate suspects involved in terrorist activities.

CBP users who also have access to IRS-NG will also have the capability to query LPR data. If LPR data is relevant to CBP's law enforcement or border security mission, CBP users will have the capability to add the results to an IRS-NG Workspace where users are able to add additional data while conducting research. IRS-NG Workspaces are limited on viewing to select groups until a user decides to publish an Intelligence Product. IRS-NG users are able to produce

Intelligence Products that could be then posted in AFI, where CBP users are able to use this information to assist with CBP's law enforcement or border security mission. A CBP user will determine if LPR data is relevant to CBP's law enforcement and border security mission and if LPR data is determined to be not relevant, it will be automatically deleted from the system, after no more than a twenty-four hour cache.

Privacy Risk: Data regarding a vehicle's location (particularly when collected over an extended period of time and retained) could potentially disclose information about an individual that is sensitive because it reveals activities that might be constitutionally protected. There is also a risk that LPR data, like other Personally Identifiable Information (PII), may be misused or inappropriately accessed for a purpose not related to a specific law enforcement activity.

Mitigation: CBP is implementing a structure that will mitigate privacy and civil liberties concerns raised by the commercial acquisition and CBP's use, storage and maintenance of LPR-related data, taking into account the growth in the availability of LPR data and the potentially sensitive information it can reveal. This structure will encompass:

1. Limited Role-Based User Access Controls: Access to commercially available LPR information will be provisioned through the CBP Entitlement System where a new entitlement role has been specifically created for this access. CBP users who require access to this sensitive dataset will proceed through a multi-level approval process. If it is determined that commercially available LPR information access is appropriate for the requestor's targeting and analytical efforts the request may be granted, or if deemed inappropriate, denied. Once LPR access is granted, CBP will provide the user an email authorizing access to LPR data, reiterating that improper use of this data may result in disciplinary action, and describing appropriate use of accessing LPR data on CBP systems laid out within this ATS PIA addendum. CBP management will ensure that requestors have met the training requirements, described below.

2. Training: CBP will require all personnel permitted to access LPR data via commercial subscription to take mandatory training for data security, privacy, information assurance, and records management on an annual basis. ATS user roles will be granted and used only for those who meet the training requirements. User roles are restricted and audited, with access predicated on a "need to know." Through user access control "entitlements," all ATS users are only permitted to access information from the source systems to which they have already been granted access. System access is managed by the ATS Entitlement System and reviewed annually to ensure the users that have access to the LPR data are recertified by a government lead.

3. Specified Purpose: When logging into ATS, AFI or IRS-NG, authorized CBP users

will see a description of the permissible uses of the system and will require a user to consent affirmatively to the requirements of accessing information on a U.S. Government system with no reasonable expectation of privacy. Each time a CBP user logs into ATS, the user must agree to the terms and conditions set forth in a splash screen before performing any query. The splash screen describes the agency's permissible uses of the system and data, and requires the user to affirmatively consent to these rules by selecting a button before proceeding. The following rules apply to the splash screen:

- The splash screen appears at each logon event; and
- Users must affirm their understanding of the rules of behavior before they are able to complete the login process and commence a query.

4. Timeframe for Query of Historical LPR Data and Retention of Results: Privacy and civil liberties concerns associated with historical searches of LPR data increase the longer the data is held by the vendor and made accessible for query. However, operational necessity may require CBP to access information sufficient to establish patterns of criminal activity over time as part of ongoing analysis or criminal investigation or to identify the movement or location of priority organizations or known associates. Therefore, CBP has determined that personnel may query up to five years of historical commercial LPR data to allow CBP personnel to conduct additional analysis and research regarding border security or law enforcement matters and access to sufficient historical data to identify trends, patterns, and potentially viable information. CBP will implement a cap within CBP systems to only allow CBP users to access LPR data within a five year period from the date of the query. CBP will only retain the results of its queries of the LPR data in ATS or other appropriate CBP systems (i.e., TECS or AFI) if the information is determined to be useful in connection with its legitimate law enforcement or border security mission. This retention will be consistent with the NARA retention schedule as specified in the relevant SORNs. CBP must manually retain the results of its queries of the LPR data that is determined to be useful in connection with its legitimate law enforcement or border security mission, while all other query results are automatically removed from the cache within twenty-four hours.

5. Use of Displays: CBP will use the capability to store license plate queries in the form of a "display" in ATS, whereby any new read of a plate on the display will result in notification to CBP. This capability will assist in the identification of a vehicle's location in near real-time, which will contribute to law enforcement efforts to apprehend individuals whose location may be connected to the vehicle's location or to know if a vehicle linked to illicit activity is approaching a port of entry. While automatic notification that an individual subject is on the move could raise privacy

and civil liberties concerns, such notification also serves an important law enforcement interest. To help reduce the potential intrusiveness of this technique, CBP policy will require displays to be updated once the enforcement matter is resolved or the individual is no longer a subject of interest. Upon creation, users will also receive notice on the importance of promptly removing license plate numbers from displays to avoid gathering LPR data without adequate justification. Users will be prompted via system notification to reexamine the entirety of their displays on a regular basis and, at a minimum, annually. Should users fail to meet this requirement, the displays will expire from the system. CBP management will review displays on a quarterly basis and verify those that are still relevant to CBP's law enforcement and border security mission.

6. Audit: ATS will provide an audit trail of each query that is made and by whom it is made. Specifically, the audit logs will capture: 1) the identity of the user initiating the query; 2) the license plate number used to query the LPR data; 3) the date and time of the inquiry; and 4) the results of the user's query. The audit trail should be generated electronically and will need to be available to, and reviewed by, CBP management or oversight personnel quarterly or more frequently to ensure the data is being used appropriately. For auditing purposes, ATS stores all query parameters, but not the query results. The vendor does not have access to these audit trails.

7. Accountability: All ATS users must undergo privacy training and obtain approval from CBP management and the ATS system owner before gaining access to ATS. ATS performs extensive auditing that records the search activities for all users. ATS has role-based access which is restricted based on a demonstrated "need to know." Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. CBP users with access to commercially available LPR information are required to complete annual security and data privacy training and their usage of the system is audited to ensure compliance with all privacy and data security requirements. CBP management will be held accountable for ensuring personnel with access to LPR data sets are properly trained and use LPR data appropriately. Periodic reviews of audit logs will confirm this is occurring. CBP management will review displays on a quarterly basis and verify those that are still relevant to CBP's law enforcement and border security mission. Auditing would be the responsibility of CBP through ATS where detailed audit logging will be implemented. DHS and/or CBP integrity offices will investigate any anomalous activity uncovered in the audit logs and CBP management will impose appropriate disciplinary action if misuse is discovered.

Privacy Risk: By accessing commercially available LPR data, CBP is now accessing data on vehicles away from the interior of the country, outside of the border zone.

Mitigation: Similar to its use of other commercially available information, CBP only accesses this information relevant to its law enforcement and border security mission, and will only retain information associated with those who cross the border and those who may be linked or connected to a person of law enforcement interest, connected to potentially criminal or other illicit activity, or for identifying individuals or entities of concern. Queries will only be associated with ongoing enforcement or border security activities. Should a CBP user use LPR information outside of these parameters, the auditing and accountability requirements will discover any misuse.

Uses of the Information

CBP identified a number of benefits from the use of LPR data from a commercial provider for its law enforcement and border security mission. Knowing the previous location(s) of a vehicle can help determine the location of subjects of criminal investigations, illicit activity, or aliens who illegally entered the United States, and thus facilitate their interdiction and apprehension. In some cases, the availability of this data may be the only viable way to find a subject. This LPR data can also show the previous movements of a subject, which may help CBP law enforcement personnel plan to apprehend while maximizing safety to the public and the officers. The vendor will provide daily updates to their data to ensure CBP has the most accurate and reliable information. LPR data from a commercial provider also allows CBP to identify connections between a vehicle and an address known for criminal activity, which may help identify individuals involved in criminal activity, permit CBP to identify those individuals who, or vehicles that, may need additional scrutiny when attempting to cross the border, or to identify and locate suspects involved in terrorist activities.

Privacy Risk: DHS defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual. The use of LPR data received from a commercial provider and used within ATS is considered PII because the license plate information is linkable to an individual. CBP recognizes there are potential privacy risks and impacts on the individual rights associated with the collection, use, and retention of LPR data. These risks include:

1) LPR data from third party sources may, in the aggregate, reveal information about an individual's travel over time, leading to privacy concerns.
2) LPR data from third party sources may, in the aggregate, provide details about an individual's private life, such as frequenting a place of worship or participating in protests and meetings, potentially implicating constitutionally-protected freedoms.
3) A license plate image or read may be incomplete or inaccurate, because the license plate is bent, dirty, or damaged or because the software reading the numbers makes an error. This can result in the misidentification of a vehicle and its occupants.

4) LPR data may accurately identify the location of a vehicle, but it may not accurately identify the whereabouts of the person that CBP is seeking.
5) LPR data may be accessed routinely, even when it is not needed.
6) LPR data may be retained for periods longer than necessary for operational purposes.
7) LPR data may be inappropriately shared with other agencies or private entities.
8) New privacy risks and impacts on individual rights may arise as technological advances create additional capabilities for LPR data collection and analysis.

Mitigation: In defining the need for this enterprise-wide solution, CBP identified requirements that will minimize the potential impact of this tool's use on individual rights and privacy. These requirements included creating a new ATS entitlement role where a user will need to demonstrate a clear "need to know" in order to be provisioned to commercially available LPR information, retention of the data consistent with the retention schedules of ATS, TECS, IRS-NG, and AFI as reflected in the relevant SORNs; internal policy controls that ensure queries are conducted only for law enforcement or border security purposes; and strong auditing requirements. CBP will require all personnel permitted to access LPR data to take mandatory training for data security, privacy, information assurance, and records management on an annual basis. When access to LPR data is granted, CBP will provide the user an email authorizing access to LPR data and stating the appropriate use of accessing LPR data on CBP systems laid out within this ATS PIA addendum. CBP recognizes the clear benefits from using LPR data to both the CBP mission and the responsibilities of DHS overall. DHS privacy policies require CBP to assess privacy risks in connection with the use of LPR technology and data, and follow the DHS Fair Information Practice Principles (FIPPs) to the extent possible. DHS civil liberties policies support the evaluation of the risks to individual rights and liberties as a result of the use of LPR technology. DHS and CBP are committed to safeguarding PII, upholding civil liberties, and reducing potential risks posed by this technology.

Notice

CBP is publishing this new ATS addendum to inform the public about LPR data CBP can access through a commercial provider. This addendum is intended to give a detailed description of what CBP is collecting, storing, and retaining, and the privacy risks that are associated with this activity. In addition, CBP has published the ATS SORN that provides public notice that CBP collects information from commercial data providers.

Privacy Risk: There is a risk that an individual may not know that his or her license plate information is accessible to CBP via a commercially available LPR information database.

Mitigation: This risk cannot be fully mitigated. While CBP is publishing this PIA to provide the public with general notice of this project, there is no way for CBP to provide specific

and timely notice to individuals that their information may become part of CBP's holdings via query of a commercial provider's data. Members of the public may not be aware that an LPR has captured their license plate information, and because CBP does not control the initial collection of this information, it cannot mitigate this risk. CBP attempts to reduce the impacts of this risk by ensuring that it only accesses information pursuant to a lead, and does not retain any information not associated with a law enforcement event.

Data Retention by the Project

CBP will be able to query up to five years of historical data to allow CBP personnel to conduct additional analysis and research regarding border security or law enforcement matters and to access sufficient historical data to identify trends, patterns, and potentially viable information. CBP will not retain in its records the results of its queries of LPR databases unless the information is determined to be useful in connection with its legitimate law enforcement or border security mission. These limitations and requirements will help to ensure CBP's access to LPR data are compatible with the purpose for which the data is sought and to minimize the risk of an over-collection of this data.

LPR data will be updated on a continuous basis from the commercial provider and reflected when queried by ATS. CBP will retain the results of its queries of the LPR data in ATS or other appropriate CBP system (e.g. TECS or AFI) if the information is determined to be useful in connection with its legitimate law enforcement or border security mission. This retention will be consistent with the NARA retention schedule as specified in the relevant SORN. The purpose of these limits is to allow CBP users seeking to conduct additional analysis and research regarding border security or law enforcement matters access to sufficient historical data to identify trends, patterns and potentially viable information or leads, while not retaining data so long as to result in the unnecessary or excessive acquisition of information. CBP will not retain in its records the results of its queries of LPR databases unless the information is determined to be useful in connection with its legitimate law enforcement or border security mission. These limitations and requirements will help to ensure access to and retention of LPR data are compatible with the purpose for which the data is sought and to minimize the risk of an over-collection of this data.

Privacy Risk: Individuals are unable to consent to the retention and use of their license plate data obtained by a commercial provider and retained in ATS.

Mitigation: Allowing a subject of law enforcement scrutiny such as a fugitive, criminal alien, or an associate of a criminal organization to be involved in whether his or her LPR information should be accessed, collected, queried, or retained from a commercially-owned repository of LPR data would significantly interfere with and undermine CBP's law enforcement mission. For this reason, CBP does not seek consent for the access to, collection, or use of LPR data. CBP queries of the commercially and law enforcement collected data are associated to

ongoing enforcement and border security activities and CBP would only retain information related to those queries. Therefore, any data CBP retains would inherently be of law enforcement value.

Information Sharing

As a matter of policy, as reflected in this PIA addendum and in the applicable Privacy Act SORNs that describe CBP's purposes for collecting data, CBP retains license plate data for those who cross the border and for those who may be linked or connected to a person of law enforcement interest, connected to potentially criminal or other illicit activity, or used for identifying individuals or entities of concern.

CBP only shares information with agencies outside of DHS consistent with the Privacy Act, including the routine uses it has published in the relevant SORNs (e.g., TECS, ATS, and AFI).

Privacy Risk: LPR information collected by CBP from a commercial vendor may be inappropriately accessed or disseminated.

Mitigation: To assist in securing LPR data against unauthorized access or use, CBP will limit the number of individuals who can access LPR data via the commercial provider. ATS and CBP intend to ensure only those who need LPR data for their mission-related purposes are able to query the data via ATS. Once an authorized query occurs, the LPR data deemed relevant to the enforcement activity will be added, as necessary, to a record or case file in the appropriate CBP system (electronic or paper) that is secure.

ATS and the vendor will maintain an immutable log of queries of the LPR data and this log will be reviewed quarterly or more frequently by CBP management or oversight personnel to ensure LPR data has been accessed for authorized purposes only. Anomalies in the audit trail that reveal inappropriate activity will be referred to the appropriate DHS or CBP integrity office for further action. The vendor supplying LPR data via ATS is employing data security technologies comparable to those required of CBP systems in order to protect the integrity of its data from hacking and other risks.

Redress

For all of the various ATS updates, redress methods remain unchanged from the original ATS PIA. Most of the information within ATS is submitted from underlying source datasets.[79] To the extent that a record is exempted in a source system, the exemption will continue to apply. Because of the law enforcement nature of ATS, DHS has exempted portions of this system from the notification, access, amendment, and certain accounting provisions of the Privacy Act of 1974. These exemptions also apply to the extent that information in this system of records is recompiled

[79] DHS/CBP-006 Automated Targeting System, 77 Fed. Reg. 30297 (May 22, 2012).

or is created from information contained in other systems of records with appropriate exemptions in place.

Privacy Risk: There is a risk that individuals cannot access or request correction of records collected and maintain by commercial providers.

Mitigation: While CBP cannot provide access or correction rights to the commercial data itself, it mitigates the redress risks posed with its collection and use of this data via the access and correction provisions of the Privacy Act and the Freedom of Information Act (FOIA). While records may be exempt from certain provisions of these laws for law enforcement purposes, CBP reviews all requests individually and takes all appropriate steps to correct its records as necessary.

Auditing and Accountability

ATS maintains robust audit trails and makes them available to appropriate CBP personnel for review. ATS will record all transactions and queries of LPR data in immutable audit logs at the individual authorized-user level and these logs are subject to review at any time by CBP oversight offices and system managers as appropriate. Specifically, system audit logs must capture: 1) the identity of the user initiating the query; 2) the license plate number used to query the LPR system; and 3) the date and time of the inquiry. This data will also be captured, thereby enhancing the usefulness of the audit trail data. The primary goal of maintaining audit logs is to deter and discover any abuse or misuse of LPR data. Any abuse or misuse of LPR data will be reported and subject to disciplinary action, as appropriate.

Before being granted access to LPR data, authorized CBP users must complete training that describes all of the above policy requirements and associated privacy, civil rights and civil liberties safeguards. This will supplement existing mandatory training required of all CBP personnel on data security, data privacy, integrity awareness, and records management.

Privacy Risk: LPR data from a commercial provider is not subject to internal DHS auditing and accountability controls; therefore, there is a risk these controls may not occur or be as robust as they would be if the vendor's system were internal to DHS. There is a risk that LPR data may be accessed routinely (even when not needed) without appropriate controls and oversight.

Mitigation: This risk can be managed by preventing over-collection and retention of the information. CBP will implement internal policies and training emphasizing the requirement to query and use LPR data only when in support of a law enforcement or border security purpose. Audit trails will capture sufficient usage data to allow the identification of CBP users who do not comply with these policies. CBP users will be required to review and validate each item on an display at least once yearly; however, employees will be required to update the displays as needed when matters are resolved or when the location of a given vehicle is no longer of law enforcement value. The fact that CBP users will have to associate queries with ongoing enforcement or border

security purpose in order to perform the queries will provide an enforcement mechanism for these requirements.

In addition, to ensure that LPR information is appropriately accessed, ATS and the vendor will capture information about the query of a license plate number. The primary goal of maintaining audit logs is to deter and discover any abuse or misuse of LPR data. Any abuse or misuse of LPR data will be reported and subject to disciplinary action, as appropriate.

ATS PIA Update Addendum 3:

New Populations Subject to ATS Vetting

3.1 International Aviation Crew Members

January 13, 2017 *(back to top)*

CBP will now retain active data and updates to the active data from the master crew member list (MCL) and master non-crew member list (MNL) in ATS for recurrent vetting. All crew members and non-crew members (e.g., air carrier employees, family members, or persons traveling onboard for the safety of the flight for commercial all-cargo flights) who may be assigned to flights operating to, from, or overflying the United States, are listed on the MCL and MNL. The lists include individuals who may be on U.S. carriers who may fly from one international point to another international point, without overflying the United States.

Existing Procedures

Per 19 CFR 122.49c, air carriers are required to submit MCL and MNL information electronically to CBP. Currently, CBP receives the information and immediately sends this information to TSA for transportation security vetting. This transmission must take place at least 48 hours in advance of the flight, with any changes being submitted at least 24 hours in advance. TSA receives the MCL and MNL information from CBP and vets the crew and non-crew members for aviation security concerns. TSA determines whether any crew or non-crew members pose security threats and must be removed from the flight.

Despite a) having independent authority to collect this information and b) receiving the information at least 24 hours prior to the flight via the Electronic Advance Passenger Information System (eAPIS),[80] CBP had opted not to retain the MCL and MNL information but instead serve as a conduit to TSA. Therefore, CBP has identified a security and passenger processing gap by not independently vetting the MCL and MNL for terrorism, border security, criminal, or immigration violations (such as visa revocations) as far in advance of the flight as possible. Currently, CBP conducts these pre-flight checks based on the standard APIS manifest transmission which occurs no later than 60 minutes prior to flight.

This current process poses several challenges. CBP may have less than one hour to assess any changes to the flight crew and non-crew members. A late determination by CBP that a crew or non-crew member should not be permitted on a flight may result in the flight being delayed or even canceled.

[80] *See* DHS/CBP/PIA-001 Advance Passenger Information System (APIS), *available at* https://www.dhs.gov/publication/advanced-passenger-information-system-apis-update-national-counterterrorism-center-nctc.

Proposed Change

Recognizing that the retention of this data may enhance vetting, strengthen security, and reduce unnecessary flight delays, the CBP National Targeting Center (NTC) seeks to retain MCL and MNL data in ATS for recurrent vetting. Specifically, the NTC seeks to:

1) Obtain a one-time transfer of active MCL and MNL data from TSA, and
2) Retain updates to the active MCL and MNL data obtained directly from air carriers as submitted through eAPIS prior to 24 hours before flight.

The NTC will update the active records with ongoing MCL and MNL data feeds. In addition, CBP's retention of the data will enhance its vetting capabilities and better enable CBP to notify operators of an issue in a timely manner, minimizing disruptions to or cancellations of flights and enhancing the protection of the aircraft, those on board, and the public.

Privacy Risks

While CBP has the authority to collect the MCL and MNL, and has opted not to do so until now, CBP Privacy has identified several privacy risks associated with this data collection that are addressed below, and via oversight mechanisms.

- Inadmissibility: If an individual appears to be inadmissible to the United States, CBP should be in a position to inform the airline as soon as possible. TSA removes individuals from the MCL or MNL on terrorism- or transportation security-related grounds only and not for immigration violations (although an immigration decision may be based on security-related grounds and thus be grounds for removal). CBP will coordinate with TSA on procedures for CBP to provide information to TSA regarding individuals who need additional review by TSA for purposes of TSA's MCL or MNL determinations. TSA will remain the authority for removing a name from the MCL or MNL.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

All of the authorities previously identified for ATS remain in effect. ATS derives its authority primarily from 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582; 8 U.S.C. § 1357; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347).

In addition, CBP also has independent authority to collect and store MCL and MNL pursuant to 19 CFR 122.49c, which requires air carriers are required to submit MCL and MNL information electronically to CBP.

All previously identified SORNs remain in effect, or are noted under the "Notice" section below.

Characterization of the Information

CBP will obtain active information and updates to active MCL and MNL information for vetting in ATS. Crew lists contain the following biographic information:

- Full name
- Gender
- Date of birth
- Place of birth
- Citizenship
- Country of residence
- Address of permanent residence
- Passport number, country of issuance, and expiration date (if required)
- Pilot certificate number and country of issuance
- Status onboard the aircraft (whether the individual is crew or non-crew)

Crew list data is received under the APIS SORN,[81] which limits retention to one year. However, CBP intends to, within one year, issue the appropriate privacy compliance documentation that will outline: 1) retaining the active MCL and MNL information, as updated by TSA and the airlines; 2) retaining for one year data concerning an individual who has been removed from TSA's MCL and MNL; 3) retaining for seven years data concerning an individual who is a potential match to a record or other derogatory information; and 4) retaining for 99 years data concerning an individual who is a confirmed match to a record or other derogatory information. In addition, information that is linked to active law enforcement records, CBP matches to enforcement activities, and/or investigations or cases may be maintained by CBP in TECS or ATS consistent with the TECS or ATS SORNs.

Privacy Risk: There is a risk that CBP's retention of MCL and MNL data is inconsistent with the terms of the original collection as specified in the APIS SORN.

[81] *See* DHS/CBP-005 Advance Passenger Information System (APIS), 80 FR 13407 (March 13, 2015), *available at* https://www.gpo.gov/fdsys/pkg/FR-2015-03-13/html/2015-05798.htm.

Mitigation: The APIS SORN provides information about CBP collecting and maintaining passenger, crew, and non-crew member data. Further, the MCL and MNL data is a subset of the APIS data already provided to CBP, but APIS data actually contains additional data elements.

However, within one year, CBP intends to issue the appropriate privacy compliance documentation to clarify and provide additional transparency to the public. The public is being made aware of this initiative through this PIA.

Uses of the Information

CBP seeks to obtain from TSA a one-time transfer of active MCL and MNL data and MCL and MNL data being retained by TSA, and retain updates to MCL and MNL data obtained directly from air carriers as submitted through eAPIS as required by 19 CFR 122.49c. The MCL and MNL data will be maintained in APIS. ATS will update the active records with ongoing MCL and MNL data feeds. In addition, CBP's retention of the data will enhance its vetting capabilities and better enable CBP to notify operators of an issue in a timely manner, minimizing disruptions to or cancellations of flights and enhancing the protection of the aircraft, those on board and the public.

Privacy Risk: There is a risk that CBP will apply targeting rules designed to identify individuals of national security concern to airline employees on the MCL.

Mitigation: This risk is partially mitigated by the fact that CBP will assess whether existing targeting rules are appropriate for individuals on the MCL and MNL. CBP will follow its current policy regarding the existing DHS oversight mechanism to ensure that targeting rules align with DHS policies.

Notice

CBP is conducting this PIA update to provide notice of CBP retention and vetting of crew member and non-crew member information. In addition, CBP will issue the appropriate privacy compliance documentation to provide notice that it is now retaining the information it has the authority to collect pursuant to 19 CFR 122.49c. There are no new privacy risks to notice identified with this initiative as CBP is already allowed to collect the information.

Data Retention by the project

CBP will retain the active MCL and MNL information, as updated by TSA and the airlines, according to the following guidelines: (1) one year for records on an individual who has been removed from TSA's MCL or MNL; (2) seven years for records on an individual who is a potential match to a record or other derogatory information; (3) 99 years for records on an individual who is a confirmed match to a record or other derogatory information. Information that is linked to active law enforcement records, CBP enforcement activities, or investigations may be maintained by CBP in TECS or ATS consistent with the TECS or ATS SORNs.

CBP will, within one year, issue the appropriate privacy compliance documentation to provide notice of this retention.

Privacy Risk: There is a risk that CBP will retain the MCL and MNL data for longer than is allowed by the retention guidelines listed above.

Mitigation: This risk is partially mitigated. To ensure compliance with these retention schedules, CBP Privacy will conduct a CPE within six months of the CBP beginning regular ingest of the data to evaluate these risks and mitigations. The results of the CPE will be shared with the DHS Privacy Office.

Information Sharing

There are no changes to information sharing from previously issued PIAs related to MCL and MNL vetting activities. TSA and CBP continue to share MCL and MNL information as mandated by law.

Redress

For all of the various ATS updates, redress methods remain unchanged from the original ATS PIA. Most of the information within ATS is submitted from underlying source datasets. To the extent that a record is exempted in a source system, the exemption will continue to apply. Because of the law enforcement nature of ATS, DHS has exempted portions of this system from the notification, access, amendment, and certain accounting provisions of the Privacy Act. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records with appropriate exemptions in place.

Privacy Risk: Individuals may not get the level of redress they desire.

Mitigation: This risk is mitigated, to the extent possible consistent with law enforcement and national security exemptions noted in the applicable SORNs. To the extent that a record is exempted in a source system, the exemption will continue to apply.

A traveler, regardless of his or her citizenship or residence, may obtain access to his or her PNR. However, records concerning the targeting rules, the responses to rules, case events, law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information, information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department, or records exempted from access by the system from which ATS ingested or accessed the information will not be accessible to the individual.

Notwithstanding the applicable exemptions, CBP reviews all such requests on a case-by-case basis. If compliance with a request would not interfere with or adversely affect the national security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of CBP in accordance with procedures and points of contact published in the applicable SORN.

Procedures for individuals to gain access to data maintained in source systems that provide data ingested into ATS would be covered by the respective SORNs for the source systems. Individuals may follow the procedures outlined in the PIAs and SORNs of the source systems to gain access to their information stored in those systems.

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a Freedom of Information Act (FOIA) or Privacy Act request in writing to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue, NW Room 3.3D
Washington, D.C. 20229

FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Specific FOIA contact information can be found at http://www.dhs.gov/foia under contacts.

If a traveler believes that CBP actions are the result of incorrect or inaccurate information, then inquiries may be directed to:

CBP INFO Center
OPA—Rosslyn
U.S. Customs and Border Protection
1300 Pennsylvania Avenue
Washington, D.C. 20229

Travelers may also contact DHS TRIP, 601 South 12th Street, TSA-901, Arlington, VA 22202 or online at www.dhs.gov/trip. Individuals making inquiries may be asked to provide additional identifying information to enable DHS to identify the record(s) at issue.

Auditing and Accountability

There are no changes to the auditing and accountability procedures for ATS as described in the previously issued ATS PIAs.

3.2 CBP Employees and Applicants

January 13, 2017 *(back to top)*

Consistent with its law enforcement and national security missions, CBP's Office of Professional Responsibility (OPR) conducts background investigations on CBP applicants, employees and contractors to determine suitability for a position with the Federal Government or for eligibility for a security clearance. OPR plans to leverage a module within ATS to perform pre-employment vetting of CBP employee and contractor applicants to facilitate this process and improve efficiencies in reviewing CBP employee applicants.

OPR's Personnel Security Division (PSD) conducts employment background investigations to support determinations of an individual's suitability for employment or continued employment, eligibility to occupy a national security position, eligibility for access to classified information, eligibility for unescorted access to DHS/CBP facilities, or access to DHS/CBP information technology systems. The initial (applicant) investigation is typically initiated pre-employment (but after a tentative job offer has been extended) for individuals seeking employment as a federal or contractor employee with CBP. Periodic reinvestigations are conducted every five years to ensure continued suitability/eligibility. Recurrent vetting and continuous evaluation is conducted between these investigations in an effort to identify derogatory information that may adversely affect the individual's suitability or eligibility for continued employment. Such vetting may be conducted as frequently as determined appropriate (e.g., daily). As part of the applicant investigation, any subsequent periodic reinvestigation, and for any recurrent vetting or continuous evaluation efforts, PSD queries a variety of databases for information associated with the subject of the investigation. As part of this data collection process, some limited queries may also be conducted on the applicant's spouse, immediate family, and/or associates. The variety and scope of the queries currently conducted is limited by the databases available for query via CBP Vetting (a CBP program that queries a variety of law enforcement databases for information based upon user-defined parameters) and by manpower limitations within PSD to conduct manual queries via TECS.

PSD uses a program called Cornerstone[82] to conduct multiple automated checks/queries via CBP Vetting. CBP Vetting provides information from the National Crime Information Center (NCIC), Nlets, Currency or Monetary Instruments Report (CMIR), Search/Arrest/Seizure (S/A/S) report, and TECS. Cornerstone also conducts automated checks of Selective Service records and records from credit bureaus. PSD supplements the automated Cornerstone checks with manual TECS queries to obtain additional information for which Cornerstone is not presently programmed to query and from additional sources (USCIS's Central Index System and DataFacts (credit reports)) not available via CBP Vetting and to delve deeper into information developed during the automated Cornerstone checks. Search parameters may include any/all of the following: name,

[82] A PIA for Cornerstone will be published in 2017.

Social Security number (SSN), date of birth (DOB), place of birth (POB), residence address, immigration document numbers (e.g., "A" and "C" numbers), Fingerprint Identification Number (FIN), and passport numbers. The following checks are currently conducted via manual checks or Cornerstone:

- Address Checks
- Border Crossing Records
- Citizenship/Immigration Checks
- CBP OPR Background Investigations
- Credit Bureau Reports (CBR)
- Criminal Record/Law Enforcement Checks
- Department of State Consular Consolidated Database (for passport status, citizenship, and visas)
- Selective Service (verification that subjects who are required to register for the Selective Service have appropriately registered)

Cornerstone presents all relevant information (including a "No Result" indicator) resulting from the automated queries/checks as a preformatted report. The CBR is presented as a separate report based on current contract requirements. PSD adjudicators review all information developed during these checks (vetting checks) to verify the information is correctly associated with the subject of the investigation and they consider all relevant information when making the final adjudicative determination as to the subject's suitability for employment.

In lieu of the checks currently conducted via Cornerstone through CBP Vetting and other manual checks conducted via TECS, PSD plans to use the Employee and Applicant Suitability and Eligibility (EASE) module of ATS to support its background investigations (including National Agency Checks (NAC)), periodic reinvestigations, and continuous evaluations. Like the query portion of Cornerstone and CBP Vetting, ATS-EASE is a system designed to facilitate the query of a variety of other systems for records/information that match user-defined parameters. ATS-EASE is not designed as a record warehouse, but does retain information regarding search parameters and queried records to meet disclosure tracking requirements and to facilitate recurrent vetting. The use of ATS-EASE automates a number of manual checks, potentially providing the PSD adjudicator with additional information associated with the subject of the background investigation. ATS-EASE will only be accessible to PSD employees and certain Office of Information and Technology (OIT) staff when needed. Data in ATS-EASE will not be searchable or accessible to other ATS users.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

Executive Order (E.O.) 10450; E.O. 12968; E.O. 13467; E.O. 13488; 5 CFR § 731; 5 CFR § 732; 5 CFR § 736; 32 CFR § 147; Security Executive Agent Directive 5; and Director of Central Intelligence Directive 6/4.

Note that these personnel security records are covered by the DHS/ALL-023 Department of Homeland Security Personnel Security Management SORN,[83] not the ATS SORN.

Characterization of the Information

OPR PSD will conduct automated queries in ATS against TECS holdings (including Watch List records), NCIC, and Nlets via ATS-EASE queries and algorithms. In addition, PSD uses ATS to query the following databases:

- Arrival and Departure Information Systems (ADIS): provides information related to subject overstays prior to obtaining citizenship based on subject provided name, DOB, Passport number, Alien Registration number, or Student and Exchange Visitor Information System (SEVIS) ID.
- ICE Enforcement Integrated Database (EID): queries apprehension records created by CBP and ICE on inadmissible aliens based on subject provided name, DOB, or Alien Registration number.
- LexisNexis: provides access to over 10,000 public record data sources on persons and businesses based on subject provided name, DOB, address, or phone number.
- OBIM Automated Biometric Identification System (IDENT): queries based on subject provided name, DOB, EID number, Passport number, or Visa number. IDENT provides biographic data on each IDENT "encounter," to include the location of the encounter, travel documents associated with the encounter, photo of subject, and whether the subject is on the biometric watch list.

Privacy Risk: There is a risk of over-collection of information since by using ATS-EASE to supplement the background investigation and suitability process, CBP has the capability to include more information than is required to determine an applicant or employee's suitability for employment.

Mitigation: CBP OPR will only use the ATS-EASE module to automate existing searches of information and databases that OPR currently reviews as part of the suitability process. CBP

[83] *See* DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010), *available at* https://www.gpo.gov/fdsys/pkg/FR-2010-02-23/html/2010-3362.htm.

uses ATS-EASE to make the process more efficient and automated, but does not present a risk of over-collection because there are no additional sources. In addition, to ensure compliance with this process, CBP Privacy will conduct a CBP Privacy Evaluation (CPE) within 12 months of the launch of ATS-EASE. The results of the CPE will be shared with the DHS Privacy Office.

Uses of the Information

In lieu of the checks currently conducted via Cornerstone through CBP Vetting and other manual checks conducted via TECS, PSD seeks to initiate checks on all individuals undergoing a CBP employment background investigation (including NAC) of applicants for CBP employment that have received a tentative offer, individuals seeking unescorted access to DHS/CBP facilities and/or access DHS information technology systems, and employees and contractors undergoing a periodic reinvestigation and/or continuous evaluation via ATS-EASE. The use of the ATS-EASE process permits additional "automated" checks to be performed thereby potentially providing the PSD adjudicator with additional information associated with the subject of the background investigation.

Privacy Risk: There is a risk that CBP will conduct suitability checks using ATS-EASE for applicants who have not been selected for employment by a hiring manager.

Mitigation: Checks related to suitability or eligibility are made utilizing information obtained from the security forms completed by applicants. Security forms are only released to applicants once they have been tentatively selected for a position and have accepted the offer. In addition, to ensure compliance with this process, CBP Privacy will conduct a CPE within 12 months of the launch of ATS-EASE. The results of the CPE will be shared with the DHS Privacy Office.

Privacy Risk: There is a risk that CBP will use more data than is necessary to determine employment suitability via the ATS-EASE module.

Mitigation: CBP OPR will only use the ATS-EASE module to automate existing searches of information and databases that OPR currently reviews as part of the suitability process. CBP uses ATS-EASE to make the process more efficient and automated, but does not present a risk of over-collection because there are no additional sources. In addition, to ensure compliance with this process, CBP Privacy will conduct a CPE within 12 months of the launch of ATS-EASE. The results of the CPE will be shared with the DHS Privacy Office.

Data Retention by the project

CBP retains personnel security data for five years after the employee's separation from the agency consistent with the NARA approved retention schedule. All queries and the query results will be retained within ATS-EASE for up to seven years to enable PSD adjudicators to review and adjudicate the potential impact of the possible hits on the suitability of each applicant and to facilitate recurrent vetting of subjects.

Privacy Risk: There is a risk that CBP will retain information for longer than the required retention period.

Mitigation: PSD will only retain information for as long as it is required for adjudicators to review and adjudicate the potential impact of possible hits on the suitability of each applicant and to facilitate recurrent vetting of subjects. PSD will retain data as per in accordance with the DHS Instruction and other guidance on personnel security and suitability.

Information Sharing

CBP's delegated investigative authority provides for the retention of investigative materials related to applicant background investigations for the greater of 15 years, or five years after the individual's separation from CBP. Subject information that is used to establish the search parameters is retained within Cornerstone for up to two years. Additionally, the raw data results from the various queries are also retained for up to two years.

All information resulting from the vetting checks (including the CBR, Cornerstone report, and screen-prints reflecting the results of all manual TECS queries (including "No Record" results)) that matched the parameters of the queries is retained in the Integrated Security Management System (ISMS).[84] Such records may include information that matched the parameters of the query but are not associated with the subject of the investigation (e.g., records for individuals with same name but that are determined not to be associated with the subject of the investigation).

The actual data from the ATS-EASE queries will not be shared with any system external to DHS.

Privacy Risk: There is a risk that unauthorized access to ATS-EASE could inappropriately expose information.

Mitigation: ATS-EASE will only be accessible to PSD employees and certain OIT staff when needed to resolve technical issues. Data in ATS-EASE will not be searchable or accessible to other ATS users. In addition, CBP OIT is constantly updating the CBP firewall to prevent unauthorized access to all CBP systems including ATS-EASE

Redress

ATS-EASE stores PII, suitability, and security clearance process tracking information related to an individual. The information is self-reported by the individual undergoing a background investigation when he or she submits his or her completed SF-85/SF-86 or e-QIP entry. Individuals are able to correct erroneous information in e-QIP before submission. Once that data has been submitted to ISMS for suitability review and clearance processing, individuals must

[84] ISMS is the DHS mandated system for tracking background investigations. For more information, please see DHS/ALL/PIA-038 Integrated Security Management System and its subsequent updates, *available at* https://www.dhs.gov/publication/dhsallpia-038b-integrated-security-management-system-isms.

contact either PSD directly, or submit a Privacy Act request via the CBP Freedom of Information Act (FOIA) Office to gain access to their records.

During the suitability determination process, each individual has the ability to address and provide mitigating information related to any derogatory information that is identified as part of his/her background investigation. Subjects are notified of any pending actions based on derogatory information and are provided a mechanism to submit mitigating information. If a derogatory finding is made, they may have appeal rights, and also the ability to request information regarding their case via the CBP FOIA office.

As identified in the Personal Security Management SORN, requests for personnel security information are made to the DHS FOIA Office, which maintains the accounting of what records were disclosed and to whom. The DHS FOIA Office submits a request for information to the CBP PSD. The PSD has the option of using the ISMS File Request module to track FOIA office requests.

Privacy Risk: Individuals may not get the level of redress to which they are entitled.

Mitigation: This risk is mitigated, to the extent possible consistent with law enforcement and national security exemptions noted in the applicable SORNs.

Notwithstanding the applicable exemptions, CBP reviews all such requests on a case-by-case basis. If compliance with a request would not interfere with or adversely affect the national security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of CBP in accordance with procedures and points of contact published in the applicable SORN.

Procedures for individuals to gain access to data maintained in source systems that provide data entered into ATS would be covered by the respective SORNs for the source systems. Individuals may follow the procedures outlined in the PIAs and SORNs of the source systems to gain access to their information stored in those systems.

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a FOIA or Privacy Act request in writing to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue, NW Room 3.3D
Washington, D.C. 20229

FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Specific FOIA contact information can be found at http://www.dhs.gov/foia under contacts.

Auditing and Accountability

There are no changes to the auditing and accountability procedures for ATS as described in the previously issued ATS PIAs. ATS-EASE will only be accessible to PSD employees and certain OIT staff when needed to resolve technical issues. Data in ATS-EASE will not be searchable or accessible to other ATS users.

3.3 ATS IntelCenter

Last updated October 3, 2018 (back to top)

ATS has traditionally served as a web-based enforcement and decision support tool used to collect, analyze, and disseminate information for the identification of potential terrorists, transnational criminals, and other persons who pose a higher risk of violating U.S. law. CBP uses ATS to augment a CBP Officer's decision-making about whether a passenger or crew member should receive additional inspection.

Social media[i] has become a powerful source of communication and interaction in the past decade and is likely to continue to evolve on a global scale as an integral component of individual identity. Increases in social media usage and internet connectivity -- as well as in the prevalence of mobile devices and their enabling of near-constant access to social media platforms -- have created myriad of new opportunities for national security adversaries or border security threats to use social media platforms for their recruitment, communications, strategy, and operations.

Open source social media content subsequently provides a wealth of information that, if properly collected and analyzed, can offer insight and assist in guiding decision-making processes to improve national security and public safety. CBP interacts on a daily basis with millions of travelers who increasingly utilize social media through a variety of available platforms. Accordingly, CBP recognizes that the effective operational use of social media can and should play a vital role in the targeting and identification of those seeking entry into the United States for the purpose of doing harm through acts of terrorism or transnational criminal activities, or those intentionally attempting to restrict or exploit lawful trade and travel.

CBP has entered into a contract with a private database vendor to test and evaluate whether ingestion of commercially available social media information into the Automated Targeting System – Targeting Framework may assist CBP in its targeting, vetting, and analysis efforts.

Privacy Impact Analysis

Authorities and Other Requirements

All of the authorities previously identified for ATS remain in effect. ATS derives its authority primarily from 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582; 8 U.S.C. § 1357; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347).

All previously identified SORNs remain in effect.

Characterization of the Information

CBP will only ingest the Social Media Handle field as part of this effort. In the event of a match, additional data fields may be uploaded into ATS.

Privacy Risk: There is a risk that may improperly identify an individual as having links to terrorism, and that CBP may take action against this individual based on erroneous information.

Mitigation: In the case of any potential "matches," CBP personnel trained in open source intelligence and research pursuant to CBP and DHS policy and guidelines would also enter database to conduct manual, directed queries on the subjects identified.

Uses of the Information

No information will be shared with the commercial provider during or after this proof-of-concept. CBP will use the information to test the potential value of incorporating open source data into CBP's vetting processes in order to better identify potential connections to known terrorist propaganda channels and actors, and may use the information to augment other data in support of operational decisions as appropriate.

Notice

CBP provides general notice of its collection of social media handles on ESTA applications in the ESTA PIA[85] and SORN.[86] In addition, ESTA applicants may review the Privacy Act Statement available on the ESTA website and are aware of CBP's collection of social media handles through their voluntary provision of the information. In addition, this PIA provides notice of ingestion of commercially sourced publicly available information into ATS.

Privacy Risk: There is a risk to notice since individuals are not provided specific, timely notice of the collection of their social media information by a third party, and the retention and use of that information by CBP.

Mitigation: This risk cannot be fully mitigated. Although CBP provides specific notice of social media information to ESTA applicants, and general notice through this PIA, CBP cannot provide specific and timely notice to individuals who are subject to CBP review as a result of information obtained. Such notice would compromise the integrity of a law enforcement matter and assist that individual in evading detection.

Data Retention by the project

Retention will not exceed 15 years, unless linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases (i.e., specific and credible threats; flights, individuals, and routes of concern; or other defined sets of circumstances).

[85] DHS/CBP/PIA-007 Electronic System for Travel Authorization, *available at* www.dhs.gov/privacy.
[86] DHS/CBP-009 Electronic System for Travel Authorization (ESTA) (September 2, 2016) 81 F.R. 60713.

Information Sharing

No information will be shared with the private sector vendor during or after this pilot. Once CBP incorporates information into a record in TECS,[87] ATS,[88] or AFI,[89] it may be viewable to other users both internal and external to CBP. User access to this information is determined by the relevant source system, will not be tagged as such, but will be incorporated along with other relevant subject information into the appropriate record if CBP personnel are able to verify the findings.

Privacy Risk: There is a risk that non-CBP users of TECS, ATS or AFI might use information derived from in a manner inconsistent with the purpose of collection.

Mitigation: This risk is partially mitigated. CBP assesses all partner agencies' missions for compatibility prior to granting access to CBP systems. Open Source information originally identified for CBP by and ingested into ATS and recorded in other systems is of law enforcement concern and CBP needs to make the information available to other agencies for law enforcement and counterterrorism purposes, as appropriate.

Redress

For all of the various ATS updates, redress methods remain unchanged from the original ATS PIA. Because of the law enforcement nature of ATS, DHS has exempted portions of this system from the notification, access, amendment, and certain accounting provisions of the Privacy Act of 1974. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records with appropriate exemptions in place.

Privacy Risk: There is a risk to redress because individuals may not be able to access social media postings (particularly if dated and/or expired) or dispute the finding that they are linked to terrorism or other suspicious activity.

Mitigation: This risk cannot be fully mitigated. CBP does not provide access to law enforcement records, including information derived from this effort, since doing so could jeopardize the law enforcement matter or enable the subject to evade detection. However, CBP continues to provide redress as described in the original ATS PIA and may correct information in its own records that are proven to be inaccurate or out of date. Furthermore, CBP personnel will conduct manual research in case of any direct matches, in order to substantiate the information identified.

Auditing and Accountability

---

[87] *See* DHS/CBP/PIA-009 TECS System *and* DHS/CBP/PIA-021 TECS System: Platform, *available at* www.dhs.gov/privacy.
[88] *See* DHS/CBP/PIA-006 Automated Targeting System, *available at* www.dhs.gov/privacy.
[89] *See* DHS/CBP/PIA-010 Analytical Framework for Intelligence, *available at* www.dhs.gov/privacy.

Access to the will be tightly controlled, and made available only to members of authorized users. Any requests for additional research into potential matches to the will be run through the appropriate CBP channels, and coordinated directly with through a consistent Point of Contact within that team. In addition, any and all CBP personnel and contractors supporting CBP missions with the need to leverage social media information and research in their operations must complete the CBP Privacy and Diversity Office's Social Media Training and sign the Social Media Rules of Behavior.

ATS PIA Update Addendum 4:

International Information Sharing Initiatives

January 13, 2017 *(back to top)*

Foreign Travel Data

Under bi-lateral arrangements with foreign governments, CBP may receive information about individuals to assist in CBP's border security mission. CBP reviews the data received pursuant to those arrangements in order to identify travelers with possible links to terrorism, wanted fugitives, missing juveniles, subjects under investigation for offences such as narcotics trafficking, currency smuggling, and weapons smuggling. CBP coordinates positive matches with CBP and other U.S. Government personnel in the United States or posted in foreign locations, as appropriate.

International Targeting Center (ITC)

The Border Five countries (Canada, the United Kingdom, Australia, New Zealand, and the United States) have established an International Targeting Center (ITC) at the National Targeting Center (NTC) facility. The ITC is designed to provide a co-located intelligence and joint targeting capability in support of Border Five data sharing and cooperative interdiction efforts. This initiative improves the ability of the Border Five countries to monitor the international movement of goods and people for security threats and illicit activity. CBP (through the NTC) and the targeting centers for the Australian Department of Immigration and Border Protection/Australian Border Force (DIBP/ABF), the Canada Border Services Agency (CBSA), the New Zealand Customs Service (NZCS), and the U.K. Border Force (UKBF) maintain liaisons at the ITC, and actively participate in its operations.

The most significant hurdle to their current collaboration and the greatest hindrance to future efforts is the lack of an efficient means to securely communicate sensitive but unclassified information – generally but not exclusively PII – between the centers. To address this challenge, CBP is developing a platform to facilitate Requests for Information (RFI), responses to RFIs, and the proactive sharing of information between partners.

Bi-Lateral Engagement with Australia, Canada, New Zealand, and the United Kingdom

The United States and its Border Five partners – Australia, Canada, New Zealand, and the United Kingdom – have long recognized the need to share information in an effort to enhance the security of our borders while continuing to facilitate the flow of legitimate travelers and cargo. In support of multiple border agreements and memorandums of understanding (MOUs), CBP and the NTC have worked with their counterpart agencies and targeting centers for DIBP/ABF, CBSA, NZCS, and UKBF. This work has covered numerous initiatives involving the exchange of traveler-related data, joint risk assessment targeting, and the sharing of lookouts based on certain types of

criminality or grounds of inadmissibility. The NTC also has an on-going liaison officer exchange with the CBSA's National Targeting Centre in Ottawa, Canada, and the UKBF's National Border Targeting Centre in Manchester, England.

Appendix A: List of Relevant Systems and SORNs, as applicable, for data available through ATS

ATS maintains copies of key elements of certain databases, including but not limited to:

- DHS/CBP-001 Import Information System (published July 26, 2016, 81 FR 48826) – which covers the Automated Commercial Environment (ACE) and Automated Commercial System (ACS)
- DHS/CBP-005 Advanced Passenger Information System (APIS) (published March 13, 2015, 80 FR 13407)
- DHS/CBP-007 Border Crossing Information (BCI) (published December 13, 2016, 81 FR 89957)
- DHS/CBP-009 Electronic System for Travel Authorization (ESTA) (published September 2, 2016, 81 FR 60713)
- DHS/CBP-022 Electronic Visa Update System (EVUS) (published September 1, 2016, 81 FR 60371)
- DHS/CBP-002 Global Enrollment System (GES) (published January 16, 2013, 78 FR 3441)
- DHS/CBP-016 Non-Immigrant Information System (NIIS) (published March 13, 2015 80 FR 13398)
- DHS/CBP-013 Seized Asset and Case Tracking System (SEACATS) (published December 19, 2008, 73 FR 77764)
- DHS/CBP-010 TECS (published December 19, 2008, 73 FR 77778)
- DHS/CBP-021 Arrival and Departure Information System (ADIS) (published November 18, 2015, 80 FR 72081)
- DHS/CBP-023 Border Patrol Enforcement Records (BPER) (published October 20, 2016, 81 FR 72601) - which covers the Border Patrol Enforcement Tracking System (BPETS) and e3 Biometrics System
- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) (published October 19, 2016, 81 FR 72080) - which covers the Enforcement Integrated Database
- DHS/ICE-001 Student Exchange and Visitor Information System (SEVIS) (published January 5, 2010, 75 FR 412)
- DHS/ALL-030 Use of the Terrorist Screening Database System of Records (published April 6, 2016, 81 FR 19988)

- Commerce/Census-012 Foreign Trade Statistics (published June 23, 2009, 74 FR 29676) - which covers the Automated Export System (AES)
- Department of State's Consular Electronic Application Center (CEAC) (published August 2, 1995, 60 FR 39469)
- Social Security Administration (SSA) Death Master File

Pointer System: ATS accesses and uses the following additional databases:

- CBP Border Patrol Enforcement Tracking System (BPETS)
- CBP's Enterprise Geospatial Information Services (eGIS)
- DHS/USVISIT-012 DHS Automated Biometric Identification System (IDENT) (June 5, 2007, 72 FR 31080)
- USCIS's Person Centric Query System (PCQS)
- DOJ/FBI-001 National Crime Information Center (NCIC) (published January 25, 2007, 72 FR 3410)
- DOJ's NCIC and the results of queries in the FBI's III
- National Insurance Crime Bureau's (NICB's) private database of stolen vehicles
- Department of State Consular Consolidated Database (CCD) PIA (published July 17, 2015)
- Nlets
- Commercial data aggregators

Manually Processed Data: ATS processes certain data in ATS and provides results back to owner of the data:

- ATS receives possible overstays from ADIS and processes them to identify additional information on whether the individual has left the country as well as whether the individual is a possible national security or public safety risk.

---

[i] Defined hereafter as, "[the subset of Open Source Intelligence explicitly including] the sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact. Social media take many forms, including but not limited to web-based communities and hosted services, social networking sites, video and photo sharing sites, blogs, virtual worlds, social bookmarking, and other emerging technologies. This definition does not apply to internal Department intranets or applications." – Derived in part from DHS Instruction 110-01-01, *Privacy Policy for Operational Use of Social Media* § IV(K) (June 8, 2012).

Per *CBP Operational Use of Social Media Directive no. 5410-003,* signed by Commissioner J. Gil Kerlikowske on

January 2, 2015, the **Operational Use of Social Media** is defined as: "[the] use of social media to collect PII for the purpose of enhancing general operational awareness, investigating an individual in a criminal, civil, or administrative context, assist in making a benefit determination about a person, assist in making a personnel determination about a CBP employee or contractor, assist in making a suitability determination about a prospective CBP employee or contractor, or for any other official CBP purpose that has the potential to affect the rights, privileges, or benefits of an individual or CBP employee or contractor. Operational use does not include the use of search engines for general Internet research, the use of social media for professional development (e.g., training and continuing education), or the use of social media for facilitating internal meetings, assigning or trading work shifts, or other internal administrative efficiencies."

The operational use of social media is broken down into the following five categories requiring differing degrees of access and supervisor approval: **Overt Engagement** – logging in to social media using DHS/CBP-branded credentials or otherwise indicating an official agency presence and engaging or interacting with individuals on or through social media; **Overt Research** – collecting information from social media without logging in or otherwise interacting with individuals through social media. Overt research does not include creating identities or credentials on social media, nor does it include concealing a government affiliation to conduct research or general, operational awareness (e.g., non-DHS affiliated IP address); **Overt Monitoring** – logging in to social media using DHS/CBP-branded credentials or otherwise indicating an official agency presence, but does not include engaging or interacting with individuals on or through social media (which is defined as Overt Engagement, above); **Masked Monitoring** – using identities or credentials on social media that do not identify a DHS/CBP affiliation, or otherwise concealing a government affiliation, to conduct research or general, operational awareness. Masked monitoring includes logging in to social media, but does not include engaging or interacting with individuals on or through social media (which is defined as Undercover Engagement, below); and **Undercover Engagement** – using identities or credentials on social media that do not identify a DHS/CBP affiliation, or otherwise concealing a government affiliation, to engage or interact with individuals on or through social media.