



**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 classes³ 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 OAG data; Social Security Administration (SSA) Death Master File; TSDB (Terrorist

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.



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 only the ATS components pertaining to cargo or conveyances rely on rules-based targeting to build

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>.



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

1. **ATS PIA Update Addendum 1: Automated Targeting System-Passenger (ATS-P) – Module Updates**
 - 1.1 [“Unified Passenger” \(UPAX\) Technology Update](#)
 - 1.2 [Facial Recognition Technology Update](#)
 - 1.3 [Transportation Security Administration \(TSA\) Secure Flight Passenger Data \(SFPD\) Vetting](#)

2. **ATS PIA Update Addendum 2: Updated Populations Subject to ATS Vetting**
 - 2.1 [CBP Trusted Traveler and Trusted Worker Populations](#)
 - 2.2 [Immigration Benefit Applicants and Petitioners](#)
 - 2.3 [Retention of Information from Electronic Devices in the Automated Targeting System-Targeting Framework](#)

3. **ATS PIA Update Addendum 3: New Populations Subject to ATS Vetting**
 - 3.1 [International Aviation Crew Members](#)
 - 3.2 [CBP Employees and Applicants](#)

4. **ATS PIA Update Addendum 4: International Information Sharing Initiatives**



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 system⁶ 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 devices⁷ 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 returned 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.

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

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



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 PIAs¹⁷ and a SORN¹⁸ 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 regulation¹⁹ 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 onboard commercial aircraft that overfly the United States in advance of the departure of those

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.



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

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. §

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.



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.

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,

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



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 TECS²⁵ 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) 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.

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>.



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. 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-

²⁶ See <https://www.tsa.gov/travel/security-screening> for additional information.



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 programs²⁷ 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;

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>.



- Uses less processing/transmission resources; and
- 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/dhsnppd-pia-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 PIA³¹ 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), available 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 created from information contained in other systems of records with appropriate exemptions in place.

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>.



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 deletes the refugee application information in ATS except for an audit log, which includes: 1) a

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>.



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 traveler whose information is being examined unless there are national security, law enforcement,

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.



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 normalized⁴⁷ 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).

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.

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 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

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

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



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:

⁴⁹ For a complete list of routine uses, see DHS/CBP-006 Automated Targeting System, System of Records, 77 FR 30297 (May 22, 2012).



- 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 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.

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).



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.



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),⁵¹ 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.

⁵¹ 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,⁵² 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.

⁵² 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 Cornerstone⁵³ 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,

⁵³ 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,⁵⁴ 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 uses ATS-EASE to make the process more efficient and automated, but does not present a risk of

⁵⁴ 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>.



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).⁵⁵ 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

⁵⁵ 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.



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



Homeland Security

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.