Privacy Impact Assessment
for the
Automated Targeting System

DHS/CBP/PIA-006(b)

June 1, 2012

Contact Point
Thomas Bush
Office of Intelligence and Investigative Liaison
U.S. Customs and Border Protection
(202) 344-1150

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

Abstract

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) operates the Automated Targeting System (ATS). As a decision support tool, ATS compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based targeting scenarios and assessments. This PIA is being conducted to notify the public about the changes in modules and expansion of access to datasets used by and stored in ATS.

This PIA is being published in conjunction with an updated System of Records Notice (SORN) that has been published in the *Federal Register*.

Overview

In order to facilitate legitimate trade and travel while managing the risk of people or cargo entering or exiting the United States who may pose a threat, DHS CBP has designed and continues to operate the Automated Targeting System (ATS).

ATS provides the following basic functionalities to support CBP in identifying individuals and cargo that need additional review across the different means or modes of travel to, through, and from the United States:

- *Comparison:* ATS compares information on travelers and cargo arriving in, transiting through, and exiting the country against law enforcement and intelligence databases to identify individuals and cargo requiring additional scrutiny. For example, ATS compares information on individuals (identified as passengers, travelers, crewmembers, or persons appearing on documents supporting the movement of cargo) trying to enter the country or trying to enter merchandise into the country against the Terrorist Screening Database (TSDB), which ATS ingests from the DHS Watchlist Service (WLS), as well as data concerning outstanding wants and warrants.
- *Rules:* ATS compares existing information on individuals and cargo entering and exiting the country with patterns identified as requiring additional scrutiny. The patterns are based on CBP officer experience, analysis of trends of suspicious activity, law enforcement cases and raw intelligence. For example, ATS might compare information on cargo entering the country against a set of scenario-based targeting rules that indicate a particular type of commodity rarely is imported from a given country.
- *Federated Query:* ATS allows users to search data across many different databases and systems to provide a consolidated view of data responsive to a query about a person or entity.

In order to execute the above three functionalities, ATS utilizes 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:

- *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 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: Automated Commercial Environment (ACE), Automated Commercial System (ACS), Arrival and Departure Information System (ADIS), Automated Export System (AES), Advance Passenger Information System (APIS), Border Crossing Information (BCI), Consular Electronic Application Center (CEAC), Enforcement Integrated Database (EID) (which includes the Enforcement Case Tracking System (ENFORCE)), Electronic System for Travel Authorization (ESTA), Global Enrollment System (GES), Non-Immigrant Information System (NIIS), historical National Security Entry-Exit Registration System (NSEERS), Seized Asset and Case Tracking System (SEACATS), U.S. Immigration and Customs Enforcement (ICE) Student Exchange and Visitor Information System (SEVIS), Social Security Administration (SSA) Death Master File, TECS, Terrorist Screening Database (TSDB) which ATS ingests from the DHS Watchlist Service (WLS), and Refused VISA data from CCD . See Appendix D for referenced SORN citations.
- *Pointer System:* ATS accesses and uses additional databases without ingesting the data, including, but not limited to: CBP Border Patrol Enforcement Tracking System (BPETS), Department of State Consular Consolidated Database (CCD), commercial data aggregators, CBP's Enterprise Geospatial Information Services (eGIS), DHS Automated Biometric Identification System (IDENT), WebIDENT, Nlets (not an acronym), DOJ's National Crime Information Center (NCIC), the results of queries in the FBI's Interstate Identification Index (III), and the National Insurance Crime Bureau's (NICB's) private database of stolen vehicles. See Appendix D for referenced SORN citations.

- *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 Arrival and Departure Information that have been identified as individuals who may have overstayed their permitted time in the United States.[1] Appendix D will be updated as necessary.

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).

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. Each of these sub-systems or modules supports the CBP officer in determining whether or not a particular individual or cargo is higher risk than other individuals or cargo. The final module looks across the different areas to find common concerns and risks. Each sub-system uses slightly different data to conduct its risk assessment, but the basic purposes as described above remain the same. Below is a summary of the sub-systems and data used for the specific purposes.

1) Automated Targeting System-AntiTerrorism (ATS-AT)

ATS-AT evaluates export information, which includes information filed electronically with AES and AESDirect. 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 the Office of Foreign Assets Control (OFAC) violations, smuggled currency, illegal narcotics, and other contraband. ATS-AT not only screens commodity information on export documents, but also screens individuals identified on those documents. ATS-AT provides a consolidated user interface to view the export information. Officers can input findings from outbound exams of exports and generate multiple reports. Further, ATS-AT allows officers to internally track shipments through custom rule criteria, review marking, and watched entity lists. Through the ATS-AT web interface CBP personnel can create *ad hoc* queries on exports.

2) Automated Targeting System-N (ATS-N)

ATS-N evaluates all cargo to identify high risk inbound cargo for examinations. ATS-N uses numerous rule and weight sets to analyze information from manifest, importer security filing, and entry data, to prioritize shipments for review, and to generate recommended targets by scoring each shipment. In some cases, ATS-N automatically places shipments on hold when they score above a specified risk threshold. ATS-N not only screens commodity information on manifest, importer security filing, and entry data, but also screens individuals, against lookouts and prior violations, who are identified on those data sources. Additionally, ATS has been updated so that if a broker or importer files a simplified entry through the Automated Broker

[1] DHS/All/PIA-041 One DHS Overstay Vetting Pilot published December 29, 2011.

Interface (ABI), ATS will screen that information and then transmit the simplified entry information to ACS and/or ACE. Through the ATS-N web interface CBP personnel can create *ad hoc* queries on cargo data. Previously, the ATS PIA identified ATS-International (ATS-I) and ATS-Trend Analysis and Analytical Selectivity Program (ATS-TAP) as modules distinct from ATS-N. In reviewing these modules and their uses, DHS/CBP determined that while these parts of ATS have a different look and feel, they provide the user with the same types of information and are used to accomplish the same purposes. As such, DHS/CBP has determined that segregation of these two separate aspects of ATS-N is no longer required.

As indicated above, the ATS-N module also includes these sub-modules:

- **ATS-I** provides designated foreign customs authorities with controlled access to automated cargo targeting capabilities. If cargo information from foreign authorities is run through the ATS-I module, it may also, consistent with applicable cooperative arrangements with that foreign authority, be retained in ATS-I and used by CBP to enhance CBP's cargo targeting capabilities. ATS-I uses the same log-in screen as ATS-N, but cargo information is screened based on a set of targeting rules defined by the participating authority without access to underlying CBP systems. Foreign customs authorities are only able to access their own data and cannot access any other data in ATS unless covered by an approved MOU.
- **Cargo Enforcement Reporting and Tracking System (CERTS)** provides CBP officers with a user-friendly, single point of entry for exam findings data. It also allows the CBP officer to query and build custom reports. CERTS establishes a historical database linking targeting reasons, risks, issues, actions, decisions, events, and past and present findings with commodities, shipping parties, and manifest information. CERTS allows trend analysis on the targeting rules based on historical enforcement information.
- **Trend Analysis and Analytical Selectivity Program (TAP) 2000** provides a user-friendly interface to quickly collect and download entry summary information to study importers and importing trends. It enables users to analyze profiles and trends, identify anomalies (unusual pricing, shifts in activity, etc.), and easily retrieve the entry summaries related to the anomalies to facilitate the detection of trade enforcement issues. The application also allows users to analyze workloads and produce resource allocation models.

As CBP continues to modernize cargo targeting, the User-Defined Rules (UDR) component allows the CBP officer to develop rules by using predefined concepts or through the matching of existing data elements in the manifest or entry.

3) Automated Targeting System-Land (ATS-L)

ATS-L evaluates previous crossing records as well as internal and external data sources for targeting at the land border. These internal and external data sources are SEVIS, CBP TECS, FBI TSDB, DOJ NCIC, Department of State's CCD, and Nlets. ATS-L stores vehicle

registration (year, make, model, and Vehicle Identification Number (VIN)) as well as registered owner information (first name, last name, date of birth, if available, and address) for U.S.-plated vehicles and biographical information on the occupants of the vehicle collected through vehicle primary processing at land border ports of entry.

4) Automated Targeting System-Passenger (ATS-P)

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 screening.

ATS-P is also used within CBP by Passenger Analytical Units (PAUs) 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 Transportation Security Administration (TSA). ATS-P provides an 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.

Additionally, ATS-P is 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 screens the visa application and provides a response to the DoS's CCD indicating whether or not derogatory information was identified by DHS about the individual. Applications of individuals for whom derogatory information is identified are referred for manual review to the appropriate agency conducting the screening. 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) case management system, after which updated information (including relevant case notes) regarding eligibility is provided to both CBP and CCD.

ATS-P is used to vet arrival and departure information received from ADIS to identify potential visa overstay candidates based on supporting data available in ATS, i.e., border crossing information, I-94, and SEVIS. In addition to identifying the list of potential overstay candidates, ATS also develops priorities based on associated risk patterns. This prioritized list of overstay candidates is then passed on to LeadTRAC, case management system 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 U.S. 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: APIS, I-94, NIIS, ESTA, BCI, TECS secondary processing, seizure and enforcement data as well as Suspect and Violator Indices (SAVI), TSDB via the Watchlist Service, and DoS's CCD to identify individuals requiring additional screening prior to entering or exiting the country.

In addition to the above, ATS-P permits specifically authorized DHS users to access PNR obtained from airlines or their travel reservation systems through the Airline Reservation Monitoring System (ResMon). ResMon interfaces with the airline reservation systems, allowing the airline reservation system to push PNR to CBP or, for certain carriers, allowing CBP to pull PNR based on a set schedule. ResMon also allows authorized CBP personnel to pull data in certain circumstances on an *ad hoc* basis, with supervisory approval, to ensure CBP has received the latest available information on specific high-risk travelers or flights.

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

5) ATS-Targeting Framework (ATS-TF)

A limited number of ATS users use the Targeting Framework (TF) to track information of targeting interest regarding passengers and cargo. The 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. If the user does not have access to the data, the search will not return any data. Information from these queries can be shared with other ATS-TF users. For example, a user at the NTC could quickly search relevant data maintained in ATS for information regarding a person of interest detained at a port of entry, and then provide the research to the port of entry. The ATS-TF provides the user with the ability to initiate research activities, 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. The ATS-TF includes workflow functionality, which allows authorized users to assign activities to other users, operating units, or ports of entry for additional processing. The ATS-TF allows the creation of projects, 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 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 activity. The ATS-TF allows users to integrate data from multiple sources and show possible relationships between entities and data elements.

Users in ATS-TF may, subject to their access permissions, query the other four modules of ATS (ATS-AT, ATS-N, ATS-L, and ATS-P) and other systems, including but not limited to those noted below, and save the results:

- Border Patrol Enforcement Tracking System - Significant Incident Report (BPETS-SIR) Module - managed by CBP
- CCD - managed by Department of State
- Commercial data aggregators
- EID - managed by ICE
- eGIS - managed by CBP
- ICE PDF Forms Generator - managed by ICE
- Social Security Administration Death Master File - managed by SSA. A copy of this file is kept in ATS-TF.
- DHS IDENT and FBI IAFIS provided through Web-IDENT - managed by ICE or E3 Biometrics - managed by CBP
- Watchlist Service - managed by DHS
- TECS - managed by CBP

The ATS-TF 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. The ATS-TF also includes sophisticated *ad hoc* reporting features for both system data and workflow metrics as well as initial reporting features through data warehouse capabilities.

The ATS-TF is made up of multiple sub-systems with distinct user interfaces specific to each user community. Each sub-system has access to all or a subset of the external data sources listed above.

- NTC interface for NTC-P, NTC-C, Port of Entry Targeting Units, and U.S. Consulates and Embassies
- Border Patrol and Intelligence Reporting System (IRS) interface for Office of Border Patrol (OBP) and Office of Air and Marine (OAM)
- Intel interface for Office of Intelligence and Investigative Liaison (OIIL)
- SIGMA interface for Office of Field Operations (OFO) users at Ports of Entry Secondary Operations
- Enforcement Link Mobile Operations – Passenger and Cargo interfaces for OFO users at Immigration Advisory Program (IAP) locations and Inbound/Outbound operations at Ports of Entry, as well as OBP users at Border Patrol Sectors
- Fraudulent Document Analysis Unit (FDAU) interface for OFO users
- Admissibility Review Office (ARO) interface for OFO users

Accessing ATS

All ATS databases and web resources are located in the National Data Center (NDC) and/or the DHS Data Centers. ATS is accessed through a web-based user interface, which enables authorized users to generate queries against ATS data on the appropriate database servers. End users communicate with web servers over the DHS infrastructure or remotely through secure encrypted devices with one-factor authentication. ATS-P is also accessible through secure-encrypted mobile devices for certain CBP officers in foreign locations and at Ports of Entry. Access to ATS is limited to those individuals with a need to know in order to carry out their official duties. Furthermore, access to specific data sets within ATS is further controlled by providing each user only those accesses required to perform his or her job. Each user's access to ATS is reviewed twice a year by the supervisor who authorized the role. Within ATS, audit trails of what information has been accessed by whom are maintained and used to support internal audits to ensure compliance with the stated purposes of the system.

Section 1.0 Authorities and Other Requirements

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

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).

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

CBP is publishing a newly updated SORN in the Federal Register to reflect the revision and expansion of ATS and to cover the official records maintained by ATS. The information contained in the source systems performing the original collection that ATS ingests from or provides a pointer to is covered by the individual SORNs of those systems as listed in Appendix D.

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

A system security plan for ATS was completed and an Authority to Operate (ATO) was granted to ATS for three years, on January 21, 2011. ATS has a FIPS 199 categorization of Confidentiality "MEDIUM," Integrity "MEDIUM" and Availability "MEDIUM." ATS processes, transmits and stores PII data.

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

Yes. Official Records (Passenger Name Records (PNR) collected under 49 U.S.C § 44909; Importer Security Filings (10+2 documentation); results of Cargo Enforcement Exams; the combination of license plate, Department of Motor vehicle registration data, and biographical data associated with a border crossing; law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information; and information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department) in this system will be retained and disposed of in accordance with a records schedule approved by the National Archives and Records Administration on April 12, 2008 and for certain PNR, the Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security, signed in December 2011. ATS collects information directly, ingests information from various systems, and accesses other systems without ingesting the data. To the extent information is ingested from other systems, data are retained in ATS in accordance with the record retention requirements of those systems, or the retention period for ATS, whichever is shortest.

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

The information contained in ATS is not covered by the Paperwork Reduction Act because ATS does not collect any information directly from the public through any paper forms. ATS does collect information from other systems, however, which in turn collect information from the public using various customs, immigration, agricultural, and admissibility forms.

Section 2.0 Characterization of the Information

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

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

ATS collects, uses, disseminates, or maintains the following information in the following modules:

ATS-AT sub-system evaluates export information, including information which is filed electronically with AES. The export data are sorted, compared to rules, and scored so that CBP officers can identify exports with aviation safety and security risks, such as FAA violations. ATS-AT also identifies the risk of exports for such violations as smuggled currency, illegal narcotics,

dual use technology, export licencing, and other contraband. ATS-AT not only screens commodity information on export documents, but also screens individuals identified on those documents.

ATS-AT may collect and store PII and data, including but not limited to the following:

- Exporter:
  - Tax ID (EIN or SSN)
  - First Name
  - Last Name
  - Address
  - City
  - State
  - Zip Code
  - Phone Number
- Office of Defense Trade Controls Registrant:
  - First Name
  - Last Name
  - Address
  - City
  - State
  - Zip Code
  - Phone Number
  - License Country
  - License Number
- Commodity:
  - VIN
  - Title State
  - Title ID
  - Bills of lading
  - Cargo manifest information (including quantity and description)

ATS-N may collect and store PII and data about incoming cargo, including but not limited to:

- Bills of lading
- Entries and importer security filings (See Appendix B for a complete listing of the ISF data elements), which identify parties in transaction by name
- Simplified entry information, including:
  - Importer of record number
  - Buyer name and address
  - Buyer Employer Identification Number
  - Seller name and address
  - Manufacturer/supplier name and address
  - Harmonized Tariff Schedule 10 digit number
  - Country of origin
  - Bill of lading/house air waybill number
  - Bill of lading issuer code
  - Entry number
  - Entry type
  - Estimated shipment value
- Tax ID (Employer Identification Number (EIN) or Social Security Number (SSN)), address and contact information including telephone and fax numbers.
- Conveyance crew information, including:
  - Name
  - Date of Birth
  - Address
  - SSN
  - Drivers License
  - Passport Numbers
- User information, including CBP internal contact information and SSN, which is masked.
- Inspection and exam results, including a narrative that can include information about the parties involved.
- Targeting information and rules that include law enforcement data about parties including name, tax ID (EIN or SSN), and address.

ATS-L accesses several external data sources for targeting at the land border. These external data sources include Nlets, NCIC, CCD, and SEVIS. The ATS-L system stores vehicle registration and biographical information collected through vehicle primary inspection. ATS-L collects and stores PII about the registered owner of the vehicle and the occupants, including but not limited to:

- Name (first and last)
- Date of birth (if available)
- Vehicle identification number (VIN) along with year, make, and model information and other vehicle registration data
- Registered owner's address
- Travel Document type and number, issue date, city, state, country

ATS-P may collect and store PII, including but not limited to the following:

- Name
- Alias
- Address
- Phone number
- Email
- License Registration
- Date of Birth
- Country of citizenship
- Country of birth
- Payment/Billing information (e.g., Credit Card or Debit Card Numbers as available)
- Gender
- Travel Document type and number, issue date, city, state, country
- Visa type and number, issue date and location
- Employment occupation code
- Fingerprint Number (FIN), where available
- Person's Physical Characteristics (height, weight, eye color, hair color, etc.)
- PNR (See appendix A for a complete PNR listing)
- SSN when provided by source system

- PII associated with targeting results or data obtained in accordance with the terms of a memorandum of understanding or other arrangement
- Ethnicity and/or Race (TECS), based on CBP officer reporting in the secondary TECS record and only if available
- Biographical and biometric information from or associated with online immigrant and non-immigrant VISA and ESTA applications, including (as available):
  - U.S. sponsor's name, address, and phone number
  - U.S. contact name, address, and phone number
  - Employer name, address, and phone number
  - E-mail address, IP address, applicant ID
  - Marital status
  - Alien number
  - SSN
  - Travel Document type and number, issue date, city, state, country
  - Tax Identification Number
  - Organization Name
  - U.S. status
  - Income information for joint sponsors
  - Education, military experience, relationship information
  - Responses to vetting questions pertaining to admissibility or eligibility

Targeting Framework may collect and store PII, including but not limited to the following:

- Name
- Address
- Alias
- Business
- Cargo information (export cargo, import cargo, express consignment with associated trade entity information)
- Country of Citizenship
- Country of Residence
- Date of Birth

- Disposition (assigned by CBP officer or agent)
- Employment Information
- PII derived from an ESTA or VISA application
- IP address
- Travel Itinerary
- Personal Identifier (marks, scars, tattoos, etc.)
- Person Type (assigned by CBP Officer or Agent)
- Place of Birth
- Property Information
- Record ID (assigned by FBI, DHS, CBP, or other agency)
- Relatives
- Remarks (entered by CBP officer or agent)
- SSN when provided by source system
- Seizure Entity
- Conveyance
- TECS lookout information
- Travel Document type and number, issue date, city, state, country
- Visa type and number, issue date and location
- Public source (e.g., Internet) information obtained by users/analysts for reference or incorporation into operational and analytical reports and/or projects

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 Arrival and Departure Information that have been identified as individuals who may have overstayed their permitted time in the United States.[2] Appendix D will be updated as necessary.

[2] DHS/All/PIA-041 One DHS Overstay Vetting Pilot published December 29, 2011.

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

ATS does not collect information directly from individuals, but rather ingests or accesses and uses information collected, generated, and stored by and in other systems. As described in section 1.2 above, ATS ingests information from the systems of records identified in section 1.2, provides a pointer to data in other systems, queries databases, and may receive data in accordance with certain cooperative arrangements with foreign governments. Additionally, some of the information maintained in ATS is created by ATS users.

The data ATS ingests comes from systems, including the following: ACE, ACS, ADIS, AES, APIS, BCI, CCD, CEAC (including Forms DS-160 and DS-260), ENFORCE, ESTA, GES, NIIS, NSEERS, SEACATS, SEVIS, TECS, TSDB-WLS, and Social Security Administration's Death Master File. Additionally, PNR collected under 49 U.S.C. § 44909 is obtained from travel reservation systems of commercial carriers. Information from Importer Security Filings is received from importers and ocean carriers. Simplified entry information is obtained from importers or brokers through ABI.

Records are accessed from BPETS, CCD, eGIS, NCIC, WebIDENT, and Nlets. Also, the results of queries in the FBI's Interstate Identification Index (III), the National Insurance Crime Bureau's private database of stolen vehicles, and commercial data aggregators are stored in ATS. ATS receives commercial data about persons and businesses as part of the analysis process for researching individuals and cargo requiring additional screening from commercial data aggregators. ATS also collects air waybill data from certain express consignment services in conjunction with specific cooperative programs.

Reports and/or projects developed in ATS-TF are created by authorized users and may include public source and/or law enforcement sensitive information uploaded by the user. Additionally, ATS records results of Cargo Enforcement Exams input by the CBP officer.

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

ATS collects PNR data directly from commercial carriers pursuant to CBP's statutory authority, 49 U.S.C. § 44909, as implemented by 19 C.F.R. 122.49d. PNR is used in conjunction with other data noted above to identify individuals requiring additional screening prior to entering the country.

ATS also collects air waybill data from certain express consignment services and other air cargo transportation providers in conjunction with specific cooperative programs.

ATS-TF uses commercial data aggregators, which provide commercial data about persons and businesses, as part of the analysis process for researching individuals and cargo requiring additional screening. ATS-TF and ATS-P users may also upload public source

information such as Internet links and documents in ATS-TF. This data are used to cross-check, confirm, and broaden the scope of information available to the user.

2.4 Discuss how accuracy of the data is ensured.

ATS relies upon the source systems listed in 2.2 to ensure that data used 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 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.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk:

ATS aggregates data from many systems, which may exceed the minimal amount necessary to achieve its missions.

Mitigation:

The nature of CBP's mission to provide effective risk management at the border requires ATS to collect any relevant information. To mitigate the risks posed in the collection of large amounts of data, CBP has imposed strict controls to maximize the security of the information that is being stored. Officers rely on data to make accurate determinations and are trained to identify inaccurate information. Data are kept in secure areas protected by armed guards. Access to ATS records is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

Privacy Risk:

Information about two different individuals with similar names and dates of birth could be mischaracterized as the same individual, thus attributing the wrong information to the wrong individual.

Mitigation:

DHS personnel are required to review and cross reference the records in ATS to improve the level of confidence and reliability in derogatory information before any action is taken against an individual.

Section 3.0 Uses of the Information

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

3.1 Describe how and why the project uses the information.

ATS-AT collects and stores the information described in 2.1, such as, exporter's name, SSN, address, and phone number to evaluate export data, including Electronic Export Information (EEI) (previously known as the Shippers Export Declaration (SED)), which is filed electronically with AES. The export data are sorted, compared to rules, and scored so that CBP officers can identify exports with transportation safety and security risks, such as FAA violations, as well as exports which may pose a risk for violation of U.S. law.

ATS-N collects and stores information described in 2.1, such as, bills of lading, entries, simplified entries, and importer security filings, which identify parties by name, tax ID (EIN or SSN), address, and contact information including telephone and fax numbers. ATS-N also leverages conveyance crew information, including name, date of birth, address, SSN (if provided), driver's license, and passport number to assist in the risk assessment of import cargo shipments aboard the conveyance. ATS-N helps to identify and select import cargo shipments that appear to have a higher likelihood of being associated with terrorism or possibly containing implements of terrorism, narcotics or other contraband in the sea, air (including mail and express mail), rail and truck modes of transportation.

ATS-L collects and stores information described in 2.1, such as, vehicle registration numbers and contact information, name, address, and travel document information for land border controls. ATS-L then parses the vehicle registration information and stores it into the ATS-L database for historical purposes and sends back the parsed results to the land border primary officers. The information sent includes vehicle registration (year, make, model, and VIN) as well as registered owner information (first name, last name, date of birth, if available, and address) for U.S.-plated vehicles.

ATS-P collects and stores information described in 2.1, such as name, address, date of birth, payment/billing information (such as credit card or debit card numbers), and passport number from the PNR, for risk assessment purposes. ATS-P augments the CBP officer's decision-making process about whether a traveler or crew member should receive additional screening. ATS-P provides an automated solution that allows CBP personnel to focus efforts on potentially high-risk travelers by eliminating labor-intensive manual comparison of traveler information or interviews with every traveler. Additionally, ATS-P receives online visa application data to provide pre-adjudication investigative screening to DoS for non-immigrant

and immigrant visa appications. ATS-P receives ESTA application data to identify potential high risk ESTA applicants. ATS-P receives ADIS data to identify potential overstay candidate leads.

ATS-TF collects and stores information described in 2.1, such as, name, SSN, address, date of birth, business, country of citizenship, country of residence, employment information, unique physical attributes (marks, scars, tattoos, etc.), and travel itinerary to authenticate travelers and cargo. CBP records in ATS-TF information on individuals and cargo that are of targeting interest.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

Yes. ATS builds a risk-based assessment 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 a score for the cargo or conveyance to subsequently identify cargo and/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-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, it compares PII described 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.

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

The principal users of ATS data are within DHS and CBP, including:

- CBP Office of Field Operations (OFO)
- CBP Office of Border Patrol (OBP)
- CBP Office of Air and Marine (OAM)
- CBP Office of Intelligence and Investigative Liaison (OIIL)
- CBP National Targeting Center (NTC)
- CBP Office of International Trade (OT)
- CBP Office of Internal Affairs (IA)
- U.S. Immigration and Customs Enforcement (ICE)
- U.S. Citizenship and Immigration Services (CIS)
- DHS Office of Inspector General (OIG)
- DHS Office of Intelligence & Analysis (I&A)
- United States Coast Guard (USCG)
- Transportation Security Administration (TSA)

The information collected through ATS may be shared with components within DHS on a need to know basis consistent with the component's mission pursuant to section 552a(b)(1) of the Privacy Act. Access to ATS is role-based and assigned according to the mission of the component and the user's need to know. Furthermore, access to specific data sets within ATS is further controlled by providing each user only those accesses required to perform his or her job.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk:

Authorized users of ATS could utilize their access for unapproved or inappropriate purposes, such as performing searches on themselves, friends, relatives, or neighbors.

Mitigation:

All ATS users must undergo privacy training and obtain approval from their supervisor and the ATS system owner before gaining access to ATS. ATS performs extensive auditing that records the search activities of all users. These audit logs are reviewed upon request and any inappropriate use will be referred to the appropriate internal investigations (such as Internal Affairs, the Joint Intake Center, or others as required) for handling. The detection of inappropriate

use will also result in the suspension of the user's access to ATS until the use can be investigated. ATS auditing capabilities are discussed in greater depth later in this document.

Audit trails are created throughout the process and are reviewed if a problem or concern arises regarding the use or misuse of the information. During the log-in process, the account owner must acknowledge his/her consent to monitoring for inappropriate use or he/she cannot access the system.

Additionally, ATS has role-based access which is restricted based on a demonstrated need to know. Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. CBP officers with access to ATS are required to complete annual security and data privacy training and their usage of the system is audited to ensure compliance with all privacy and data security requirements.

Privacy Risk:

One potential risk to individuals from the use of ATS is that a traveler, conveyance, or cargo in which an individual has an interest may be referred to secondary inspection even though that traveler, conveyance, or cargo does not present any risk of harm to the United States and has not committed or been associated with any violation of U.S. law.

Mitigation:

Referral to secondary inspection, as necessary, permits an officer to intercede and resolve mis-identifications, and to clarify information associated with an individual's travel document records. Determinations in secondary regarding admissibility are made by a CBP officer or supervisor. Secondary processing is a necessary component of CBP's admissibility determination for each person arriving in the United States when admissibility cannot be determined at primary inspection. Generally, other than random referrals employed periodically as an internal control to ensure consistent procedures, decisions to refer travelers to secondary inspection are made by a CBP Officer. As a decision support system, ATS operates according to the rules within the system that were created in parallel with the policies and procedures governing the CBP inspection process. The review, analysis, and training of the officer making a decision regarding admissibility at secondary inspection provides the greatest mitigation to the risk that information in ATS may be improperly obtained or inappropriately accessed or used.

Likewise, all cargo shipments arriving in or exported from the United States are subject to further review or physical inspection to determine that the shipment poses no threat and that the shipment is in compliance with all applicable U.S. laws and regulations. This data review or physical inspection of the cargo shipment serves a similar function in allowing CBP or other applicable regulatory agency to determine that no violation has occurred.

Section 4.0 Notice

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

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

ATS does not collect any information directly from individuals. ATS does collect and maintain PNR data derived from commercial carrier reservation/departure control systems, as indicated in the SORN for ATS published at the same time as this PIA in the Federal Register and discussed above at paragraph 1.1. DHS provides extensive notice about its use of PNR on both the CBP and DHS Privacy Office websites. In addition, airlines provide general notification about their obligation to report PNR in the contract of carriage.

In cases where an individual has a concern during an interaction with a CBP officer, the CBP officer may provide the individual with a copy of the fact sheet, "If You Experience Problems With Your Arrival in the U.S." (See Appendix C), which provides general information concerning CBP's border enforcement mission and responsibilities and specific information concerning where to direct inquiries about CBP's actions or the information collected. In addition, travelers may also contact DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip. Individuals making inquiries should provide as much identifying information as possible regarding themselves to identify the record(s) at issue.

Most of the information that ATS uses is collected from government data sources. Notice was provided through the applicable source SORNs and PIAs (where applicable), as well as through the publication of the laws and regulations authorizing the collection of such information. This information is collected and stored in the source systems of record, is collected for compatible purposes, and would be collected with or without ATS. See Appendix D for listing of the relevant SORNs.

This information is collected by CBP primarily for law enforcement purposes related to the entry and exit from the United States of people, cargo, and conveyances; use of this data also facilitates legitimate trade and travel.

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

Generally, the decision whether to travel to or from, or to import and/or export goods/merchandise into or out of the United States is within the discretion of the individual. United States law requires individuals seeking to enter the country to identify themselves and

demonstrate admissibility to the United States; likewise, persons seeking to import or export goods and merchandise into or out of the United States are required to provide certain information to allow CBP to determine whether the goods/merchandise may enter the United States, and are in compliance with relevant export requirements, as applicable.

ATS does not require individuals to provide information beyond that authorized by law. This information is captured by the source systems (e.g., AES, ACS and/or ACE, and TECS) and used by ATS to efficiently and expeditiously identify persons, conveyances, and cargo that may pose a concern to law enforcement, resulting in further review by appropriate government officers.

While ATS does not collect information directly from individuals, it employs information obtained from persons by these source systems. The only way an individual can decline to provide information is to refrain from traveling to, from, through, or over the United States or by not bringing in, shipping, or mailing any goods/merchandise to, through, or from the United States.

Any consent individuals may grant is controlled by the source systems described in earlier sections. Because the submission of information is required in order to travel to, from, through, or over the United States or to bring in, ship, or mail any goods/merchandise to, through, or from the United States, restrictions on CBP use and sharing of accessed information are limited by legal requirements set forth in the Privacy Act, the Trade Secrets Act, the uses published in SORNs and, for certain PNR, the U.S.-EU Passenger Name Record Agreement. Consent to store or use this information must be done in accordance with the above legal requirements.

Opportunities for individuals to consent to particular uses of information are addressed using the processes defined by the source systems. As most information collected by these systems is mandated by law, there is effectively no consent mechanism other than the choice whether to travel or ship items.

Many commercial carriers have provided their own notice to customers concerning the requirement to provide PNR.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk:

There is a risk that the individual may not know that the information is being used by ATS in the ways described.

Mitigation:

CBP has published the SORN for ATS and this PIA (as well as previous versions) to increase transparency of its operations. Regarding PNR, CBP and DHS have provided information via the DHS Privacy and CBP websites and other mechanisms to effectively notify the traveling public. Additionally, CBP and DHS have drafted language regarding PNR for commercial carriers to include in their privacy statements so as to provide further transparency.

Many air carriers have provided their own notice to customers concerning the uses and transmission of PNR.

Section 5.0 Data Retention by the Project

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

Official Records (including PNR collected under 49 U.S.C. § 44909; Importer Security Filings (10+2 documentation); results of Cargo Enforcement Exams; the combination of license plate, Department of Motor vehicle registration data, and biographical data associated with a border crossing; law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information; and information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department) in this system will be retained and disposed of in accordance with a records schedule approved by the National Archives and Records Administration on April 12, 2008. ATS collects information directly, ingests information from various other systems, and accesses other systems without ingesting the data. To the extent information is ingested from other systems, data are 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 below. The retention period for PNR will be subject to the following further access restrictions and masking requirements: ATS users with PNR access will have access to PNR in an active database for up to five years, with the PNR depersonalized and masked after the first six months of this period. After the initial five-year retention period in the active database, the PNR will be transferred to a dormant database for a period of up to ten years. Within the dormant database, PNR will be accessible for criminal matters for up to five years but will remain available for counter-terrorism purposes for the full duration of its 15-year retention. PNR in dormant status will be subject to additional controls including the requirement of obtaining access approval from a senior DHS official designated by the Secretary of Homeland Security. Furthermore, PNR in the dormant database may only be repersonalized in connection with a law enforcement operation and only in response to an identifiable case, threat, or risk. Such limited access and use for older PNR strikes a reasonable balance between protecting this information and allowing CBP to continue to identify potential high-risk travelers. Notwithstanding the foregoing, information maintained only in ATS that is linked to a specific case or investigation will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

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. This 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.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk:

Data may be retained too long.

Mitigation:

ATS retains data according to the SORN requirements of the system from which the data was obtained. PNR is retained for five years in an active state and ten years in a dormant state. However, users will only be able to view the PII in PNR for six months. After six months PII will be masked and require each user to obtain supervisory approval before unmasking the PII. All of these accesses are logged and reviewed to ensure compliance. These retention periods permit CBP to perform the necessary assessment results from rules, because much of the targeting environment relies upon historical data. Acknowledging the changing nature of the targeting environment and the sensitivity of the data, CBP archives data after the prescribed period to further protect data that may not be immediately required, but may become relevant within the retention period.

ATS maintains the assessment results from rules together with a record of which rules were used to develop the risk assessment. This assessment and related rules history associated with developing assessment results from rules are maintained for up to fifteen years to support ongoing targeting requirements. Notwithstanding this limitation, information maintained in ATS that is linked to an active law enforcement matter will be retained for the duration of that law enforcement matter.

Nonetheless, the touchstone for data retention is the data's relevance and utility. Accordingly, CBP will regularly review the retention period for ATS to ensure its continued relevance and usefulness. If these reviews demonstrate that certain data is no longer relevant and useful, CBP will revise the retention period and delete the information.

All assessment results from rules need to be maintained because assessment results from rules for individuals who are deemed low risk will be relevant if their risk attributes change in the future, for example, if new terrorist associations are identified. Additionally, certain data maintained by ATS may be subject to shorter retention limitations pursuant to separate arrangements. The adoption of shorter retention periods may not be publicly disclosed if DHS concludes that disclosure would affect operational security.

Privacy Risk:

ATS may retain data longer than the source system.

Mitigation:

In general, ATS has implemented controls that delete data in ATS if such data are deleted in the source system. For data that has been identified by a CBP Officer in ATS as having law enforcement relevance, the record may be maintained longer than allowed for in the source system. In the relevant retention schedules of the source systems, DHS has allowed for the retention of records of law enforcement relevance.

Section 6.0 Information Sharing

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

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Non-DHS requesters may only access information in the various modules of ATS if there is a specific information sharing arrangement in place between DHS and the outside entity. Each arrangement defines the nature of the outside access to or sharing of ATS information, including the scope of the ATS information being access or shared and the legal basis upon which they receive it. Depending on the information sharing arrangement, the non-DHS requesters may be provided direct access to ATS and in other instances the non-DHS requester may be provided access through a CBP/DHS user of ATS, as described below.

CBP provides varied levels of access to ATS-N for imported commodities to the following:

- Air cargo transportation providers including express consignment carriers receive access to receipt acknowledgments from CBP regarding document review and official government cargo hold messages from users of ATS.
- Consumer Product Safety Commission and other members of the CBP hosted Commercial Targeting and Analysis Center (CTAC) receive direct system access to cargo and commodity targeting information pertaining to import safety to fulfill the targeting mandate of the Consumer Product Safety Improvement Act of 2008, and other import safety statutes.

CBP may provide the results of passenger screenings to the following:

- Various law enforcement task forces outside of DHS that require queries to be run against ATS data (for example, the FBI-led Joint Terrorism Task Force) in response to a specific threat or to analyze specific travel routes of concern.
- Law enforcement and counterterrorism agencies, in response to direct requests and authorized releases.

- National Counterterrorism Center (NCTC) in the event that the National Targeting Center-Passenger (NTC-P) nominates an individual for inclusion within the TSDB.
- Terrorist Screening Center (TSC) – Interface (DHS data transfer) for Outbound departures where there is a potential match to the TSDB.
- Other domestic and foreign agencies consistent with the published Routine Uses in the SORN.

CBP provides online visa application pre-adjudication investigative screening results to DoS, including justification for the determination.

ATS allows all users, including non-DHS users, to access source system data consistent with their user roles. In some instances users have less access through ATS than their direct access to the source system. Agencies with this type of access include:

- Department of Justice (Federal Bureau of Investigation, Drug Enforcement Administration, Bureau of Alcohol, Tobacco, Firearms, and Explosives)
- Department of State (Diplomatic Security and Consular Affairs)
- U.S. Department of Commerce (Bureau of Industry and Security)
- U.S. Department of Agriculture (this access includes viewing of specific USDA rule sets and assessment results from rules)
- Department of Health and Human Services (U.S. Food and Drug Administration FDA) (limited to FDA personnel working at NTC in support of FDA Prior Notice requirements)
- United States Postal Service

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

As stated in section 1.2 of this document, the Privacy Act SORN that applies to ATS was revised and expanded in conjunction with this PIA. In updating the ATS SORN, DHS reviewed it to ensure that the sharing described above is compatible with the purpose of the system.

6.3 Does the project place limitations on re-dissemination?

External users of ATS must meet the terms and conditions of the arrangements permitting their access to ATS in order to obtain and maintain access. Generally, CBP requires that the external users employ the same or similar security and safeguarding precautions as employed by CBP and only use the data for legitimate purposes. For CBP, ATS has role-based security. Users from other government organizations must use the ATS interface to access the system where access is limited via a user profile/role. ATS user roles are highly restricted and audited. Application access is restricted in the form of role based access, which is based on a demonstrated need to know. Users may not re-disseminate information without prior express written consent by CBP.

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

Information shared outside of the Department is tracked through the use of the DHS-191, Accounting of Disclosure Form, or a Memorandum of Understanding (MOU). CBP and DHS users of ATS prepare a DHS-191 form each time they share PII from ATS outside of DHS. The ATS-P module automatically generates an electronic copy of the DHS-191 in each instance of sharing when PNR data are shared from ATS. CBP and DHS share information from ATS pursuant to the terms of an arrangement for access to one or more of the modules of ATS, or in accordance with the language of a letter of authorization, which facilitates the sharing of a limited number of records from ATS in response to a request for assistance from another law enforcement agency.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk:

Information may be shared under inappropriate circumstances.

Mitigation:

Risks related to sharing of information outside DHS, including any potential risk of further dissemination of information by the external agency to a third agency, are mitigated through arrangements governing access to ATS by external parties and sharing of ATS information with external parties. Each arrangement defines the nature of the outside access to or sharing of ATS information, including the scope of the ATS information being accessed or shared and the legal basis upon which they receive it. The arrangements generally require the external party accessing or receiving information to employ measures relating to security, privacy, and safeguarding of information that are equivalent or comparable to measures employed by DHS. As a general matter, the arrangements also stipulate that any further dissemination of ATS information by the receiving party to a third party is subject to prior authorization by CBP. Lastly, CBP emphasizes that, within each arrangement, each external user is provided with training designed to ensure that data accessed through ATS is safeguarded and secured in an appropriate manner and that dissemination restrictions are observed, consistent with applicable laws and policies.

Section 7.0 Redress

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

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

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. To the extent that a record is exempted in a source system, the exemption will continue to apply. Despite the exemptions taken on this system of records, CBP and DHS are not exempting the following records from the access and amendment provisions of the Privacy Act: PNR collected pursuant to its statutory authority, 49 U.S.C. § 44909, as implemented by 19 CFR 122.49d; Importer Security Filing (10+2 documentation) information; and any records that were ingested by ATS where the source system of records already provides access and/or amendment under the Privacy Act. A traveler, regardless of his or her citizenship or residence, may obtain access to his or her PNR, but 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
FOIA Division
799 9th Street NW, Mint Annex
Washington, DC 20229-1177

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*.

While DHS has exempted ATS from the access and amendment provisions of the Privacy Act, individuals may make a request to view their records. When seeking records about oneself from ATS or any other CBP system of records, the request must conform to the Privacy Act regulations set forth in 6 CFR part 5. An individual must first verify their identity, meaning that they must provide full name, current address, and date and place of birth. The request must include a notarized signature or be submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, forms for this purpose may be obtained from the Director, Disclosure and FOIA, http://www.dhs.gov/foia or 1–866–431–0486. In addition, the following should be provided:

- An explanation of why the individual believes DHS would have information on them,
- Details outlining when they believe the records would have been created, and
- If the request is seeking records pertaining to another living individual, it must include a statement from that individual certifying his/her agreement for access to his/her records.

Without this bulleted information, CBP may not be able to conduct an effective search, and the request may be denied due to lack of specificity or lack of compliance with applicable regulations.

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

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, DC 20229

Travelers may also contact DHS TRIP, 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip. Individuals making inquiries should provide as much identifying information as possible regarding themselves to identify the record(s) at issue.

As many of the records used by ATS come from TECS, CBP has instituted an Officer-initiated function in TECS to address certain issues pertaining to some records that may contain conflicting information. This function is referred to as the Primary Lookout Override (PLOR) function. The PLOR function was developed to assist travelers who are erroneously designated for secondary inspections because they possess a characteristic similar to a person of interest. PLOR allows CBP Officers to override certain TECS Records where a similar biographical trait exists between the traveler and another person who is the subject of a TECS Record, provided that the non-subject traveler is able to provide a unique characteristic that differentiates him or her from the person of interest. The PLOR procedures require supervisory approval before a PLOR record may become active. All such amended transactions are logged by TECS and attributed to the authorized user performing the correction. This includes any required supervisory approval.

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

Upon request, CBP officers will provide the fact sheet, "If You Experience Problems With Your Arrival in the U.S.," that provides information on appropriate redress (See Appendix C). The redress procedure provides the ability to correct data in the source systems, including ATS. Additional information is available on DHS's website. The source system SORNs also provide information on accessing and amending information collected through those systems as discussed in 7.1 and 7.2, above.

7.4 Privacy Impact Analysis: Related to Redress

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

Mitigation: Redress procedures allow for correction of individual-provided data.

As set forth in the SORN published in conjunction with this PIA, DHS has exempted portions of ATS from the access, amendment, and certain accounting provisions of the Privacy Act (specifically 5 U.S.C. §§ 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I); (e)(5), and (8); (f) and (g)) pursuant to 5 U.S.C. §§ 552a (j)(2). Additionally, DHS has exempted this system from the following provisions of the Privacy Act, pursuant to 5 U.S.C. §§ 552a(k)(1) and (k)(2): 5 U.S.C. §§ 552a(c)(3); (d)(1), (2), (3), and (4); (e)(1), (e)(4)(G) through (I); and (f). DHS and CBP, however, will consider each request for access to records maintained in ATS to determine whether or not information may be released. Also, as noted above in paragraph 7.1, individuals may, pursuant to the FOIA, seek access to information for which ATS is the source system or which originates from another government source system and as a matter of CBP policy, redress may also be requested in the manner described above in paragraph 7.2.

However, individuals, regardless of nationality, country of origin or place of residence who believe their PNR has been used in an inappropriate manner may seek redress, including but not limited to, through the DHS Traveler Redress Inquiry Program.

Additionally, DHS Privacy Office published guidance on February 11, 2011 specifically on identifying, processing, tracking, and reporting on requests for amendment to records submitted to DHS under the Privacy Act.[3]

Section 8.0 Auditing and Accountability

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

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

The controls in place to ensure that information is handled in accordance with the above described uses include:

Misuse or Breach of ATS: ATS has role-based access. All user groups will have access to the system defined by the specific user's profile and limited through reference to the determined rights and responsibilities of each user. Access by users, managers, system administrators, developers, and others to the ATS data is defined in the same manner and employs profiles to tailor access to mission or operational functions. ATS user roles are highly restricted and audited. Access is restricted in the form of role based access, which is based on a demonstrated need to know. Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. All ATS users with access to ATS are required to complete security and data privacy training on an annual basis and their usage of the system is audited to ensure compliance with all privacy and data security requirements.

ATS is hosted at the NDC and/or the DHS Data Centers. Both are secure, access-controlled facilities with physical security and protective services 24 hours a day, 7 days a week. The computer room is further restricted to a controlled list of authorized individuals. The building floors are occupied by CBP personnel who are required to pass a security background investigation. No non-government system hosting is involved.

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

All ATS users are required to take annual security training such as the "CBP Sensitive Security Information," "CBP IT Security Incident Response Training," "CBP Safeguarding Classified National Security Information," and "CBP IT Security Awareness and Rules of Behavior Training" through the online DHS - Virtual Learning Center (VLC). Each of the VLC security trainings covers what constitutes PII and how to handle PII.

[3] *Privacy Policy Guidance Memorandum 2011-01*

The Targeting and Analysis Systems Program Office (TASPO) maintains a master list of all ATS users to ensure an accurate record.

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

ATS user access is restricted in the form of role-based access assigned based on the user's role. Users cannot assign their roles to any other user, nor can they elevate their own rights within the system. User access is enforced by the user's role-based access, and roles are assigned only after supervisor request, process owner approval, and appropriate security checks have been confirmed.

Initial requests for access to the system are routed from the user through the supervisor to the System Administrator for processing. Need to know determinations are made at both the supervisor and Process Owner level. If validated, the request is passed on to the System Administrator. System Security Personnel are tasked to determine the user Background Investigation (BI) status. Once the BI is validated, the user's new profile changes are implemented. The user, supervisor, and Process Owner are notified via email that the request has been processed along with instructions for the initial login. These records are maintained by CBP. Profile modification requests follow the same process as for an initial request. If an individual has not used the system for more than 90 days, that individual's access will be denied and the same procedures as noted above must be completed to renew access. In addition, access is periodically reviewed by the Process Owner to ensure that only appropriate individuals have access to the system.

ATS user access is highly restricted and audited based on a demonstrated need to know. Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. Data are retrieved through authorized users logging in to the CBP network remotely using encryption and passwords to access the ATS web-based interface.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, and new access to the system by organizations within DHS and outside?

There are arrangements in place to govern access to or sharing of information from ATS. These agreements or arrangements are drafted by the business owners with input from the program managers. Arrangements that involve PII are sent to the CBP Privacy Officer for review and to DHS for final approval in accordance with procedures developed by the DHS Information Sharing Governance Board.

Responsible Officials

Laurence Castelli
CBP Privacy Officer
Office of International Trade
U.S. Customs and Border Protection
Department of Homeland Security

Thomas Bush
Executive Director
Targeting Division
Office of Intelligence and Investigative Liaison
U.S. Customs and Border Protection
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix A: PNR Data Types

PNR may include the following types of information when available:*

1. PNR record locator code
2. Date of reservation/ issue of ticket
3. Date(s) of intended travel
4. Name(s)
5. Available frequent flier and benefit information (*i.e.*, free tickets, upgrades)
6. Other names on PNR, including number of travelers on PNR
7. All available contact information (including originator of reservation)
8. All available payment/billing information (*e.g.*, credit card number)
9. Travel itinerary for specific PNR
10. Travel agency/travel agent
11. Code share information (*e.g.*, when one air carrier sells seats on another air carrier's flight)
12. Split/divided information (*e.g.*, when one PNR contains a reference to another PNR)
13. Travel status of passenger (including confirmations and check-in status)
14. Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote (ATFQ) fields
15. Baggage information
16. Seat information, including seat number
17. General remarks including Other Service Indicated (OSI), Special Service Indicated (SSI) and Supplemental Service Request (SSR) information
18. Any collected APIS information (*e.g.*, Advance Passenger Information (API) that is initially captured by an air carrier within its PNR, such as passport number, date of birth and gender)
19. All historical changes to the PNR listed in numbers 1 to 18

*Not all carriers collect PNR and of those that do collect this data, not all collect the same sets of PNR data. Not all carriers maintain the same sets of information for PNR and an individual PNR is not likely to include information for all possible categories.

Appendix B: Importer Security Filing Data Elements

The Importer Security Filing (ISF) must contain the following items, in addition to the Vessel Stow Plan (VSP) and the Container Status Message (CSM):

1) Manufacturer (or supplier);

2) Seller (*i.e.*, full name and address or widely accepted business number such as a Data Universal Numbering System (DUNS) number);

3) Buyer (*i.e.*, full name and address);

4) Ship to party (full name and/or business name and address);

5) Container stuffing location;

6) Consolidator (stuffer);

7) Importer of record number/Foreign Trade Zone applicant identification number;

8) Consignee number(s);

9) Country of origin; and

10) Commodity Harmonized Tariff Schedule of the United States (HTSUS) number.

Alternatively, for shipments consisting entirely of Freight Remaining on Board (FROB) or shipments consisting of goods intended to move through the United States, ISF Importers, or their agents, must submit the following five elements, unless an element is specifically exempted:

1) Booking party (*i.e.*, name and address);

2) Foreign port of unlading;

3) Place of delivery;

4) Ship to party; and

5) Commodity HTSUS number.

Appendix C: Fact Sheet—"If You Experience Problems With Your Arrival in the U.S."

U.S. Customs and Border Protection

If You Experience Problems With Your Arrival in the U.S.

FACT SHEET

United States Customs and Border Protection (CBP) is an agency within the Department of Homeland Security. Our job is to keep America's borders safe and secure while encouraging legitimate travel and trade. We must keep terrorists and their weapons out of the country while enforcing hundreds of laws designed to protect our citizens, border, and commerce. To accomplish this, CBP officers must screen all arriving people, goods and vehicles to make sure they meet all requirements for entry into the United States.

Authority to search

The Congress of the United States has authorized CBP to enforce all homeland security-related laws and laws of other federal agencies at the border and to conduct searches and examinations necessary to assure compliance with those laws. CBP's broad authority therefore allows us to conduct searches of people and their baggage, cargo, and means of transportation entering the United States.

The laws and regulations we enforce include (but are not limited to):

- Admissibility of aliens
- Importation of agriculture, plant, and animal products
- Importation of goods, animals and produce
- Transportation and reporting of currency and other monetary instruments
- Exportation of weapons and items subject to defense trade controls

What to expect during a CBP examination

The CBP officer may request specific, detailed information about your travel, may inspect your baggage, or may conduct a personal search.

If you are subject to inspection, you should be treated in a courteous, dignified, and professional manner. However, please keep in mind that this is a law enforcement environment, and travelers who are intent on breaking the law will attempt to find out what the officer is doing in order to avoid detection. For this reason, our CBP officers may not answer specific questions about an examination that is underway. You may always ask to speak with a CBP supervisor.

Why you may be chosen for an inspection

You may be subjected to an inspection for a variety of reasons including but not limited to:

- Your travel documents are incomplete, or you do not have the proper documents or visa;
- You have previously violated one of the laws CBP enforces;
- You have a name that matches a person of interest in one of the government's enforcement databases; or
- You have been selected for a random search.

A search may not be made on any discriminatory basis (e.g., solely based on race, gender, religion, ethnic background).

Collection of personal information

CBP collects information about people traveling into and out of the United States. This includes basic biographic data, travel documents and their unique identifiers, where the traveler is staying in the U.S., and the planned purpose for the traveler's visit. This information may be collected from a traveler at a port of entry, or, in the case of international air and sea travel, it may be collected before a traveler's arrival in or departure from the U.S. This information is used to determine

For more information, visit the CBP.gov website or contact the Office of Public Affairs at 202–344–1770.

10/07

the admissibility of aliens and to effectively and efficiently enforce U.S. laws at the border. CBP also collects pertinent data about businesses, vehicles, aircraft, and vessels related to the laws we enforce.

CBP receives and shares this type of information as appropriate with other federal, state, and local agencies. CBP may query its record systems to ensure compliance with U.S. customs, immigration, agriculture, and other federal laws. For example, our border enforcement systems provide officers with access to information on outstanding watches and warrants; stolen vehicles, vessels or firearms; license information; criminal histories; and previous federal inspections.

Privacy protection

CBP stores all data we collect in secure computer systems on a secure network. CBP is committed to protecting travelers' personal data consistent with U.S. laws. We have privacy protections in place to properly safeguard this data. We also have policies in place to prevent misuse and those policies are regularly evaluated and updated to ensure continued security and protection.

Customer service contacts

1. Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP)

DHS TRIP provides a single point of contact for individuals who experience repeated referrals for security screenings or who believe that they have been denied boarding or entry into the United States because of inaccurate or incorrect information about them in law enforcement records, or because they have been confused with someone who is a concern to U.S. authorities. For more information on TRIP or to submit an inquiry, please see the DHS TRIP website at: http://www.dhs.gov/trip.

If you are uncertain as to the source of the information or the agency responsible for maintaining the information causing your travel concern, then you should begin your inquiry with DHS TRIP.

2. Customer Service Center

If you know you were stopped or delayed because of a previous incident involving CBP or one of its legacy components (Immigration and Naturalization Service, U.S. Border Patrol, or U.S. Customs Service) but believe that this matter should no longer be a factor in your clearing customs and immigration, you may ask CBP to review and possibly amend your records. If you want to ask why you were stopped, then you may ask CBP through its Customer Service Center.

CBP's Customer Service Center responds to travelers' general or specific questions or concerns about a CBP examination. You can contact us in one or three ways:

- **Telephone:** at or (877) 227-5511 for U.S. callers during the hours of 8:30 a.m. to 5:00 p.m. Eastern Time;
- **Online:** through the "Questions" tab at http://www.cbp.gov.xp.cgov/travel/customerservice; or
- **Mail:** by sending a letter to CBP Customer Service Center (Rosslyn VA), 1300 Pennsylvania Avenue NW, Washington, DC 20229.

When you contact the Customer Service Center for a written response, you should provide in writing: your full name, address, date of birth, and a copy of the photo page of your passport (or other photo identification if you do not have a passport). In addition, you should provide as detailed an explanation of the problem and why you think it should no longer be a concern and your records should be amended.

3. Freedom of Information Act (FOIA) and Privacy Act (PA) Requests

If you have concerns about being stopped or delayed and would like CBP to provide you with a copy of the records in its possession that pertain to you, then you may submit a request to CBP at the following address:

U.S. Customs and Border Protection
1300 Pennsylvania Avenue, NW,
Attn: Mint Annex Building, FOIA Division
Washington, DC 20229

You should provide your full name, address, date of birth, and any other personal identifying information you believe might be helpful in locating records related to your inquiry or resolving your concern. After receiving your request, we will research the matter, and respond with copies of those records, which may be disclosed. Please note that neither the FOIA nor the PA is intended to provide a mechanism for asking questions of CBP. FOIA and PA requests are intended to provide access to certain records under the control of the agency from which you request them. If you have questions concerning, for example, the reason why an action was taken, then you should contact DHS TRIP or CBP's Customer Service Center.

Appendix D: List of Relevant Systems and SORNs, where applicable, for data available through ATS

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

- DHS/CBP-001 Automated Commercial Environment (ACE) (published January 19, 2006, 71 FR 3109)
- DHS/CBP-015 Automated Commercial System (ACS) (published December 19, 2008, 73 FR 77759)
- Commerce/Census-012 Foreign Trade Statistics (published June 23, 2009, 74 Fed. Reg. 29676) - which covers the Automated Export System (AES)
- DHS/CBP-005 Advanced Passenger Information System (APIS) (published November 18, 2008, 73 FR 68435)
- DHS/CBP-007 Border Crossing Information (BCI) (published July 25, 2008, 73 FR 43457)
- Department of State's Consular Electronic Application Center (CEAC) (published August 2, 1995, 60 FR 39469)
- DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE) (published May 3, 2010, 75 FR 23274) - which covers EID
- DHS/CBP-009 Electronic System for Travel Authorization (ESTA) (published November 2, 2011, 76 FR 67751)
- DHS/CBP-002 Global Enrollment System (GES) (published April 21, 2006, 71 FR 20708)
- DHS/CBP-016 Non Immigrant Information System (NIIS) (published December 19, 2008, 73 FR 77739)
- DHS/CBP-013 Seized Asset and Case Tracking System (SEACATS) (published December 19, 2008, 73 FR 77764)
- DHS/ICE-001 Student Exchange and Visitor Information System (SEVIS) (published January 5, 2010, 75 FR 412)
- Social Security Administration (SSA) Death Master File
- DHS/CBP-010 TECS (published December 19, 2008, 73 FR 77778)
- DHS/USVISIT-001 Arrival and Departure Information System (ADIS) August 22, 2007 (72 FR 47057)
- DHS/ALL-030 Use of the Terrorist Screening Database System of Records (published July 6, 2011, 76 FR 39408)

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

- CBP Border Patrol Enforcement Tracking System (BPETS)
- Department of State Consular Consolidated Database (CCD) (PIA available at http://www.state.gov/documents/organization/93772.pdf)
- Commercial data aggregators
- CBP's Enterprise Geospatial Information Services (eGIS)
- DHS/US-VISIT-0012 DHS Automated Biometric Identification System (IDENT) (June 5, 2007, 72 FR 31080)
- Nlets (formerly National Law Enforcement Telecommunications System)
- DOJ/FBI-001 National Crime Information Center (NCIC) (published September 28, 1999, 64 FR 52343, January 31, 2001, 66 FR 8425, and January 25, 2007, 72 FR 3410)

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

- ATS receives possible overstays from USVISIT 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. [4]

[4] DHS/All/PIA-041 One DHS Overstay Vetting Pilot published December 29, 2011.