Privacy Impact Assessment
for the

Automated Targeting System

August 3, 2007

Contact Point
Roland Suliveras
Office of Field Operations
U.S. Customs and Border Protection
(202) 344-3780

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
703-235-0780

Abstract

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) has developed the Automated Targeting System (ATS). ATS is one of the most advanced targeting systems in the world. Using a common approach for data management, analysis, rules-based risk management, and user interfaces, ATS supports all CBP mission areas and the data and rules specific to those areas. CBP is updating and republishing this PIA in conjunction with the System of Records Notice (SORN) and the Notice of Proposed Rulemaking (NPRM) for Privacy Act exemptions published on August 6, 2007 in the *Federal Register* at 72 FR 43650 (SORN) and 72 FR 43567 (NPRM) .

Introduction

ATS is an intranet-based enforcement and decision support tool that is the cornerstone for all CBP targeting efforts. As a decision support tool ATS compares traveler, cargo, and conveyance information against intelligence and other enforcement data by incorporating risk-based targeting scenarios and assessments. CBP uses ATS to improve the collection, use, analysis, and dissemination of information that is gathered for the primary purpose of targeting, identifying, and preventing potential terrorists and terrorist weapons from entering the United States. Additionally, ATS is utilized by CBP to identify other violations of U.S. laws that are enforced by CBP. In this way, ATS allows CBP officers charged with enforcing U.S. law and preventing terrorism and other crime to focus their efforts on travelers, conveyances, and cargo shipments that most warrant greater scrutiny. ATS standardizes names, addresses, conveyance names, and similar data so these data elements can be more easily associated with other business data and personal information to form a more complete picture of a traveler, import, or export in context with previous behavior of the parties involved. Traveler, conveyance, and shipment data are processed through ATS, and are subject to a real-time rule based evaluation.

ATS provides equitable treatment for all individuals in developing any individual's risk assessment score because ATS uses the same risk assessment process for any individual using a defined targeting methodology for a given time period at any specific port of entry.

ATS consists of six modules that provide selectivity and targeting capability to support CBP inspection and enforcement activities.

- ATS-Inbound – inbound cargo and conveyances (rail, truck, ship, and air)
- ATS-Outbound – outbound cargo and conveyances (rail, truck, ship, and air)
- ATS-Passenger (ATS-P) – travelers and conveyances (air, ship, and rail)
- ATS-Land (ATS-L) - private vehicles arriving by land
- ATS - International (ATS-I) - cargo targeting for CBP's collaboration with foreign customs authorities
- ATS-Trend Analysis and Analytical Selectivity Program, (ATS-TAP) (analytical module)

Five of these modules are operational and subject to recurring systems' maintenance. They are: the ATS cargo modules, import, and export (ATS Inbound and ATS Outbound); the ATS-Passenger module; the ATS-Land module; and ATS-Analytical module. The ATS-International module is being developed to support collaborative efforts with foreign customs administrations.

As a legacy organization of CBP, the U.S. Customs Service traditionally employed computerized screening tools to target potentially high-risk cargo entering, exiting, and transiting the United States. ATS originally was designed as a rules-based program to identify such cargo; it did not apply to travelers. ATS-P became operational in 1999 and is critically important to CBP's mission. ATS-P allows CBP officers to determine whether a variety of potential risk indicators exist for travelers and/or their itineraries that may warrant additional scrutiny. ATS-P maintains Passenger Name Record (PNR) data, which is data provided to airlines and travel agents by or on behalf of air passengers seeking to book travel. CBP began receiving PNR data voluntarily from air carriers in 1997. Currently, CBP collects this information as part of its border enforcement mission and pursuant to the Aviation and Transportation Security Act of 2001 (ATSA).

ATS receives various data in real time from the following different CBP mainframe systems: the Automated Commercial System (ACS), the Automated Export System (AES), the Automated Commercial Environment (ACE), and the Treasury Enforcement Communications System (TECS). TECS includes information from the Federal Bureau of Investigation Terrorist Screening Center's[1] Terrorist Screening Database (TSDB) and other government databases regarding individuals with outstanding wants and warrants and other high risk entities. ATS collects certain data directly from commercial carriers in the form of a Passenger Name Record (PNR). Lastly, ATS also collects data from foreign governments and certain express consignment services in conjunction with specific cooperative programs.

ATS accesses data from these sources, which collectively include electronically filed bills of lading, entries, and entry summaries for cargo imports; shippers' export declarations and transportation bookings and bills for cargo exports; manifests for arriving and departing passengers; land-border crossing and referral records for vehicles crossing the border; airline reservation data; nonimmigrant entry records; and records from secondary referrals, incident logs, suspect and violator indices, seizures, information from the TSDB, and other government databases regarding individuals with outstanding wants and warrants and other high risk entities.

In addition to providing a risk-based assessment system, ATS provides a graphical user interface (GUI) for many of the underlying legacy systems from which ATS pulls information. This interface improves the user experience by providing the same functionality in a more rigidly controlled access environment than the underlying system. Access to this functionality of ATS uses existing technical security and privacy safeguards associated with the underlying systems.

---

[1] The TSC is an entity established by the Attorney General in coordination with the Secretary of State, the Secretary of Homeland Security, the Director of the Central Intelligence Agency, the Secretary of the Treasury, and the Secretary of Defense. The Attorney General, acting through the Director of the FBI, established the TSC in support of Homeland Security Presidential Directive 6 (HSPD-6), dated September 16, 2003, which required the Attorney General to establish an organization to consolidate the Federal Government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes. The TSC maintains the Federal Government's consolidated terrorist watch list, known as the TSDB.

As part of an ongoing effort to review and update system of records notices, CBP published a new SORN for ATS in the *Federal Register* on November 2, 2006 located at 71 FR 64543. This system of records was previously covered by the legacy TECS SORN. Based on comments received in response to the November 2, 2006 notice, CBP is issuing a revised SORN, which amends the retention period, access provisions, and other substantive areas of the prior notice and provides further notice and transparency to the public about the functionality of ATS. Those revisions are discussed in the SORN published August 6, 2007 at 72 FR 43650.

ATS System Overview

Currently, ATS consists of six modules that focus on exports, imports, passengers and crew (airline passengers and crew on international flights, passengers and crew on sea carriers), private vehicles crossing at land borders, and import trends over time. ATS assists CBP officers at the borders effectively and efficiently identify cargo, individuals, or conveyances that may present additional risk to the United States.

Specifically, ATS uses information from CBP's law enforcement databases, the TSDB, information on outstanding wants or warrants, information from other government agencies, and risk-based rules developed by analysts to assess and identify high-risk cargo, conveyances, and travelers that may pose a greater risk of terrorist or criminal activity and therefore should be subject to further scrutiny or examination.

A large number of rules are included in the ATS modules, which encapsulate sophisticated concepts of business activity that help identify suspicious or unusual behavior. The ATS rules are constantly evolving to both meet new threats and refine existing rules. ATS applies the same methodology to all individuals to preclude any possibility of disparate treatment of individuals or groups. ATS is consistent in its evaluation of risk associated with individuals and is used to support the overall CBP law enforcement mission.

These rules are based on investigatory and law enforcement data, intelligence, and past case experience.

- *ATS-Inbound* is the primary decision support tool for inbound targeting of cargo. This system is available to CBP officers at all major ports (air/land/sea/rail) throughout the United States, and also assists CBP personnel in the Container Security Initiative (CSI) and Secure Freight Initiative (SFI) decision-making process. ATS Inbound provides CBP officers and Advance Targeting Units (ATU) with an efficient, accurate, and consistent method for targeting and selecting high-risk inbound cargo for intensive examinations. ATS-Inbound increases the effectiveness of CBP officers dealing with imported cargo by improving the accuracy of the targeting of weapons of mass effect, narcotics or other contraband, commercial fraud violations, and other violations of U.S. law. ATS-Inbound processes data pertaining to entries and manifests against a variety of rules to make a rapid automated assessment of the risk of each import. Entry and manifest data is received from the Automated Manifest System (AMS), Automated Broker Interface (ABI), the Automated Commercial System and, its successor system, the Automated Commercial Environment (ACE).

- *ATS-Outbound* is the outbound cargo targeting module of ATS that assists in identifying exports which pose a high risk of containing goods requiring specific export licenses, narcotics, or other contraband or exports that may otherwise be in violation of U.S. law. ATS-Outbound uses Shippers' Export Declaration (SED) data that exporters file electronically with CBP's AES.[2] The SED data extracted from AES is sorted and compared to a set of rules and evaluated in a comprehensive fashion. This information assists CBP officers with targeting and/or identifying exports with potential aviation safety and security risks, such as hazardous materials and Federal Aviation Administration (FAA) violations. In addition, ATS-Outbound identifies the risk of specific exported cargo for such export violations as smuggled currency, illegal narcotics, stolen vehicles or other contraband.

- *ATS-Passenger* (ATS-P) is the module used at all U.S. airports and seaports receiving international flights and voyages to evaluate passengers and crewmembers prior to arrival or departure. It assists the CBP officer's decision-making process about whether a passenger or crewmember should receive additional screening prior to entry into or departure from the country because the traveler may pose a greater risk for violation of U.S. law. ATS-P's screening relies upon the following databases, Advanced Passenger Information System (APIS), Non Immigrant Information System (NIIS), Suspect and Violator Indices (SAVI), the Department of State visa databases, the PNR information from the airlines, TECS crossing data, TECS seizure data, information from the consolidated and integrated terrorist watch list maintained by the TSC. ATS-P processes available information from these databases to develop a risk assessment for each traveler. The risk assessment is based on a set of national-and user-defined rules that are comprised of criteria that pertain to specific operational/tactical objectives or local enforcement efforts. Unlike in the cargo environment, ATS-P does not use a score to determine an individual's risk level; instead, ATS-P compares PNR and information in the above-mentioned databases against lookouts and patterns of suspicious activity identified through past investigations and intelligence. This risk assessment is an analysis of the threat-based scenario(s) that a traveler matched when traveling on a given flight. These scenarios are drawn from previous and current law enforcement and intelligence information.

- *ATS-Land* (ATS-L) is a module of ATS that provides for the analysis and rule-based risk assessment of private passenger vehicles crossing the nation's borders. By processing and checking the license plate numbers of vehicles seeking to cross the border, ATS-L allows CBP officers to cross-reference the TECS crossing data, TECS seizure data, and State Department of Motor Vehicle (DMV) data[3] to employ the weighted rules-based assessment

[2] The Shipper's Export Declaration (SED), Commerce Form 7525-V, is used to compile the official U.S. export statistics for the United States and for export control purposes. The regulatory provisions for preparing, signing and filing the SED are contained in the Foreign Trade Statistics Regulations (FTSR), Title 15, Code of Federal Regulations (CFR) Part 30.

[3] DMV data to support ATS-L is obtained from a government source, National Law Enforcement Telecommunications System (NLETS). DMV data obtained to support ATS-L will only be used to support land border targeting applications. Access to the ATS-L application and the DMV data it uses are limited to DHS users including CBP officers and Border Patrol Agents. No other use or dissemination of DMV data will be performed by CBP.

system of ATS. In this way ATS-L provides, within seconds, a risk assessment for each vehicle that assists CBP officers at primary booths in determining whether to allow a vehicle to cross without further inspection or to send the vehicle for secondary evaluation.

- *ATS-International* (ATS-I) is being developed to provide foreign customs authorities with controlled access to automated cargo targeting capabilities and provide a systematic medium for exchanging best practices and developing and testing targeting concepts. The exchange of best practices and technological expertise can provide vital support to other countries in the development of effective targeting systems that can enhance the security of international supply chains and fulfill the objective of harmonizing targeting methodologies. If 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 by CBP to enhance CBP's targeting capabilities.

- *ATS-Trend Analysis and Analytical Selectivity* (ATS-TAP,) improves CBP's ability to examine, locate, and target for action violators of US laws, treaties, quotas, and policies regarding international trade. ATS-TAP offers trend analysis and targeting components. The trend analysis function summarizes historical statistics that provide an overview of trade activity for commodities, importers, manufacturers, shippers, nations, and filers to assist in identifying anomalous trade activity in aggregate.

ATS supports the decision-making process and reinforces the role of the trained professionals making independent decisions necessary to identify violations of U.S. law at the border.

Section 1.0 Information Collected and Maintained

The following questions are intended to define the scope of the information requested as well as the reasons for its collection as part of the system, rule, and/or technology being developed.

1.1 What information is to be collected?

Generally, ATS collects and maintains personally identifiable information relating to name, risk assessment, and the internal system rules upon which the assessment is based and Passenger Name Record data obtained from commercial carriers.

In order to build the risk assessment, ATS uses data obtained from other governmental information systems including: electronically filed bills of lading, entries, and entry summaries for cargo imports; shippers' export declarations and transportation bookings and bills of lading for cargo exports; manifests for arriving and departing passengers and crew; airline reservation data; nonimmigrant entry records; and records from secondary referrals, CBP incident logs, suspect and violator indices, state Department of Motor Vehicle Records (for vehicle license plate numbers), TSDB, seizure records, and law enforcement lookout information.

- ATS-Inbound: Collects information about importers, cargo, and conveyances used to facilitate the importation of cargo into the United States. This includes personally identifiable information (*e.g.*, name, address, birth date, government issued identifying records, where available and applicable) concerning individuals associated with imported cargo: brokers, carriers, shippers, buyers, sellers, and crew.

- ATS-Outbound: Collects information about exporters, cargo, and conveyances used to facilitate the exportation of cargo from the United States. This includes personally identifiable information (*e.g.*, name, address, birth date, government issued identifying records, where available and applicable) concerning individuals associated with exported cargo: brokers, carriers, shippers, buyers, sellers, and crew.

- ATS-P: Collects information about passengers and crew entering or departing the United States. This data includes passenger and crew manifests (through APIS, which also includes crew data for flights overflying the U.S.), immigration control information, and PNR data. The PNR data may include such items as name, address, flight, seat number, and other information collected by the airline in connection with a particular reservation (Appendix B contains a list of types of information collected from a PNR). Not all carriers capture the same amount of information; the number of items captured may even vary among individual PNRs from the same carrier.

- ATS-L: Collects information about vehicles and persons entering the U.S. at land border ports of entry. This data includes license plate numbers for vehicles entering the United States, vehicle, and registered owner data (derived from state DMV records). ATS-L receives license plate number via TECS. Using that license plate number, ATS-L then queries DMV data via National Law Enforcement Telecommunications System (NLETS) to obtain registration information for that vehicle (name, date of birth, address of the registered owner).

- ATS-I: Provides an interface for access to cargo targeting functionality by foreign customs authorities, as defined in separate information sharing arrangements. ATS-I permits foreign customs authorities to view restricted cargo information in ATS-Inbound coming from or to their nations, according to their own queries, or to add data, separately collected from their own systems, to be targeted against the developed screening queries. ATS-I collects trade data and related personally identifiable information (*e.g.*, name, address, birth date, government issued identifying records, where available and applicable) collected by foreign customs authorities, in accordance with the applicable arrangement negotiated for data sharing and access with that customs authority.

- ATS-TAP: Aggregates entry summary declarations to enable analysis of trends in trade activity and selective targeting of summary transactions related to identified anomalies.

ATS obtains information from the various sources identified in Appendix A. The information in these data files is cross-referenced between databases to correlate and augment information pertaining to an individual for purposes of screening or risk assessing. ATS permits user analysis of these risk assessments for purposes of targeting persons and commodities

requiring further scrutiny or examination. As part of this risk assessment, ATS incorporates information from CBP's law enforcement databases, the Federal Bureau of Investigation Terrorist Screening Center's the Terrorist Screening Database (TSDB), information on outstanding wants or warrants, information from other government agencies regarding high-risk parties.

1.2 From whom is information collected?

ATS does not collect information directly from individuals. The information maintained in ATS is either collected from private entities providing data in accordance with U.S. legal requirements (*e.g.*, PNR from air carriers regarding individual passengers) or is created by ATS as part of the risk assessment and associated rules.

The information used by ATS to build the risk assessment is collected from government data sources and from private entities providing data in accordance with U.S. legal requirements or other applicable arrangements (*e.g.* inward and outward manifests, merchandise entries).

1.3 Why is the information being collected?

Personally identifiable information is collected to ensure that people, conveyances, and cargo entering or exiting the United States comply with all applicable U.S. laws. Relevant data, including personally identifiable information, is necessary for CBP to assess effectively and efficiently the risk and/or threat posed by a person, a conveyance operated by person, or cargo handled by a person, entering or exiting the country. CBP's ability to identify possible violations of U.S. law or other threats to national security would be critically impaired without access to this data. ATS permits all such information to be applied more efficiently and effectively to support both CBP's law enforcement mission, while also facilitating legitimate travel, trade, commerce, and immigration.

As noted in the System of Records Notice the purposes for use of PNR in ATS-P are (a) to prevent and combat terrorism and related crimes; (b) to prevent and combat other serious crimes, including organized crime, that are transnational in nature; (c) to prevent flight from warrants or custody for crimes described in (a) and (b) above; (d) wherever necessary for the protection of the vital interests of a data subject or other persons; (e) in any criminal judicial proceedings; or (f) as otherwise required by law.

The purposes of ATS (other than PNR in ATS-P) in addition to those purposes listed above for PNR in ATS-P are (a) to perform targeting of individuals, including passengers and crew, focusing CBP resources by identifying persons who may pose a risk to border security or public safety, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law, (b) to perform a risk-based assessment of conveyances and cargo to focus CBP's resources for inspection and examination and enhance CBP's ability to identify potential violations of U.S. law, possible terrorist threats, and other threats to border security; and (c) to otherwise assist in the enforcement of the laws enforced or administered by DHS, including those related to counterterrorism.

1.4 How is the information collected?

The information that ATS uses is collected from government data sources (*e.g.*, other government databases) and from entities providing data in accordance with U.S. legal requirements or other applicable arrangements (*e.g.*, PNR from air carriers regarding individual passengers). ATS does not collect additional information directly from individuals.

Personally identifiable information that is collected through other government databases, such as TECS, ACE, ACS, AMS, APIS, AES, TSDB, and National Crime Information Center (NCIC), is collected and stored in source systems of records. This information is collected by CBP in those systems to assist it in carrying out its law enforcement responsibilities relative to the importation or exportation of cargo, or the entry or exit of persons from the United States.

1.5 What specific legal authorities/arrangements/agreements define the collection of information?

There are numerous customs and immigration authorities authorizing the collection of data regarding the import and export of cargo, the entry and exit of conveyances and travelers.[4] Additionally, ATS-Outbound and ATS-Inbound supports CBP functions mandated by Title VII of Public Law 104-208, which provides funding for counter-terrorism and drug law enforcement. ATS-Outbound also supports functions arising from the Anti-Terrorism Act of 1997, the Clinger-Cohen Act, the Paperwork Reduction Act (PRA), and the Privacy Act. Both the PRA and the Privacy Act impose requirements and limits upon the government regarding the collection of information directly from persons; however, the flexibility of ATS's design and cross-referencing of databases permits CBP to employ information collected from persons through multiple systems, for additional compatible uses within a secure information technology system.

The risk assessments for cargo that are conducted through ATS are also mandated under section 203 of the "Security and Accountability for Every Port Act of 2006" (SAFE Port Act) (P.L. 109-347) (October 11, 2006). ATS-P helps satisfy CBP's responsibilities arising from the Aviation and Transportation Security Act of 2001, which mandated the electronic transmission of APIS and PNR information to CBP; these requirements are vital to the protection of national security and were enacted as a result of the terrorist attacks of September 11, 2001, which revealed significant deficiencies in the area of aviation security. ATS-TAP was developed in response to analytical deficiencies identified in a Congressional GAO audit. ATS-TAP also addressed mandates to modernize import and export processing systems and to provide automated tools that assist in the administration and enforcement of international trade agreements. ATS-TAP gives CBP the capability to issue periodic compliance reports to Congress, set priorities for allocating available resources, and improves fiscal management associated with revenue collection.

[4] See, *e.g.*, 19 U.S.C. 482, 1431, 1433, 1461, 1496, 1499, 1581-1583; 8 U.S.C. 1221,1357 and 49 U.S.C. 44909.

1.6 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

The privacy risks associated with the maintenance of the information in ATS include: the information may not be accurate or timely because it was not collected directly from the individual, the information could be used in a manner inconsistent with the privacy policy stated at the time of collection, and/or the individual may not be aware that the information is being used by ATS for the stated purposes and/or a negative CBP action could be taken in reliance upon computer generated information in ATS that has been skewed by inaccurate data.

To mitigate these privacy risks, CBP has done the following:

Accurate and Timely Information. The system generates a risk assessment; however, no action will be taken unless the information has been reviewed by a CBP officer trained in the interpretation of the information and familiar with the environment in which the information is collected and used. The ATS system supports CBP officers in identifying individuals or cargo that may pose a risk of violating U.S. laws or otherwise constitute a threat to national security, but it does not replace their discretion to determine whether the individual or cargo should be permitted to enter or exit the country and/or be subject to additional examination. If personally identifiable information is believed by the data subject to be inaccurate, a redress process has been developed and the individual is provided information about this process during the secondary review. See Section 7 of this PIA.

Consistency with the stated privacy policy. Prior to inclusion of information from system of records notices other than ATS, CBP reviews the routine uses and purposes statements to ensure that the purposes for which the information was collected and used are consistent with the law enforcement purposes of ATS. CBP officers are trained on the limited uses for which the information may be used in connection with their official duties.

Lack of awareness of the use of information. In order to increase transparency, CBP published a SORN in the Federal Register on August 6, 2007 (72 FR 43650) and this PIA as means of informing individuals about the specific elements of ATS (ATS was previously considered a part of TECS). Additionally, before information may be used in ATS the Privacy Act system of records notice must be reviewed by CBP to ensure the use is consistent with the stated purposes.

Automatic negative determination. As part of CBP's inspection policies and procedures no adverse action is taken by CBP with respect to an individual, cargo or conveyance until the relevant information is reviewed by a well-trained CBP officer. This risk is further mitigated by the fact that any person or merchandise seeking to enter or depart the U.S. border may be subject to inspection by CBP in accordance with its broad border search authority.

Section 2.0 Uses of the System and the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

Authorized CBP officers and other government personnel located at seaports, airports, and land border ports around the world use ATS to support targeting, inspection, and enforcement related requirements.

ATS is a critical tool that enables CBP to improve the collection, use, analysis, and dissemination of information to target, identify, and prevent potential terrorists and terrorist weapons from entering the United States and identify other violations and violators of U.S. law. The automated nature of ATS greatly increases the efficiency and effectiveness of the officer's otherwise manual and labor-intensive work, and thereby helps facilitates the more efficient movement of legitimate cargo and people while safeguarding the border and the security of the United States. In this way ATS facilitates international trade and travel while enhancing homeland and border security.

ATS also provides a simulation environment, with respect to its cargo and passenger modules, for CBP analysts to test rules and targeting concepts as a means of refining the support ATS gives to CBP's border enforcement mission. An additional benefit of this simulation environment is the ability of analysts to reduce the incidence of false positives or mis-identifications by more finely distinguishing the rules criteria, thereby further facilitating lawful trade and travel.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

Yes. ATS builds a risk-based assessment for persons, cargo and conveyances based on criteria and rules developed by CBP. ATS maintains the risk assessment together with a record of which rules were used to develop the risk assessment. It is worth clarifying, however, that only the ATS components pertaining to cargo rely on rules-based "scoring" to identify cargo shipments of interest. Travelers identified by risk-based targeting scenarios identified through the ATS-P are not assigned scores.

The ATS rules and resulting risk assessments 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. The Targeting Framework environment is a workflow and reporting function that separately allows users to track risk assessment effectiveness and create various reports permitting a more comprehensive analysis of CBP's enforcement efforts. The Manager's Dashboard update to the GUI is a reporting function that separately allows managerial users to create various reports permitting a more comprehensive analysis of CBP's enforcement efforts

ATS- Inbound and ATS- Outbound conduct data mining as defined by Congress[5] and reported on in the DHS Privacy Office Data mining report to Congress. ATS-P, which maintains

[5] Conference Report on HR 5441, DHS Appropriations Act, House Report No. 109-699, Sept. 28, 2006, H7784, at

PNR does not meet the Congressional definition of data mining. ATS risk assessments are always based on predicated and contextual information. As noted above unlike in the cargo environment, ATS-P does not use a score to determine an individual's risk level; instead, ATS-P compares PNR and information in the above-mentioned databases 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.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

ATS relies upon the source systems 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 the CBP officer will take action to correct that information, when appropriate. ATS monitors source systems for changes to the source system databases. Continuous source system updates occur in real-time or near real-time from TECS, ACE, AMS, APIS, ACS, AES, TSDB, and NCIC. When corrections are made to data in source systems, ATS updates this information immediately and only the latest data is used. In this way, ATS integrates all updated data (including accuracy updates) in as close to real-time as possible.

Furthermore, in the event personally identifiable information (such as PNR) used by and/or maintained in ATS is believed by the data subject to be inaccurate a redress process has been developed, about which the individual is provided information during examination at secondary. See Section 7 of this PIA. Additionally, under the ATS System of Records Notice, CBP permits the subject of PNR or his or her representative to obtain access and request amendment of the PNR in accordance with the Privacy Act of 1974.

To the extent information that is obtained from another government source (for example, DMV data that is obtained through NLETS) is determined to be inaccurate, this problem would be communicated to the appropriate government source for remedial action.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

The privacy risks associated with the use of the information maintained in ATS include: additional inspection and misuse of data by users.

H7815. uses the following definition for "data mining": "... a query or search or other analysis of 1 or more electronic databases, whereas – (A) at least 1 of the databases was obtained from or remains under the control of a non-Federal entity, or the information was acquired initially by another department or agency of the Federal Government for purposes other than intelligence or law enforcement; (B) a department or agency of the Federal Government or a non-Federal entity acting on behalf of the Federal Government is conducting the query or search or other analysis to find a predictive pattern indicating terrorist or criminal activity; and (C) the search does not use a specific individual's personal identifiers to acquire information concerning that individual.

Additional Inspection. One risk to individuals from the use of ATS is to be referred to secondary inspection. Every individual is subject to inspection under U.S. law, so, all individuals are always at risk of referral to secondary inspection—ATS, through its refinement of targeting criteria seeks to reduce this risk for the average traveler to that of merely random chance. As a decision support system, ATS operates according to the rules within the system that were created to parallel the policies and procedures that govern the CBP inspection process to ultimately protect individual's privacy rights. To the extent that an individual may be referred to secondary inspection based, in part, upon an analysis of information derived through ATS, this PIA and the SORN for ATS as well as the PIAs and SORNs for the source systems, from which ATS draws information, provide the greatest mitigation to the risk that information may be improperly obtained or inappropriately accessed or used.

ATS offers equitable risk assessment using a secure encrypted network; however, it is the policies and procedures and laws that govern the inspection process that ultimately protect individual privacy rights. The professionalism applied by CBP officers serves to further protect individual privacy rights.

Misuse or Breach of ATS. ATS has role-based access. ATS User roles are highly restricted and audited. Access is restricted in the form of Mandatory Access Control, 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. CBP officers 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.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

The information initially collected in ATS is used for entry, exit, and in-transit screening and risk assessment purposes. Records in this system will be retained and disposed of in accordance with a records schedule to be approved by the National Archives and Records Administration.

ATS both collects information directly, and derives other information from various systems. To the extent information is collected from other systems, data is retained in accordance with the record retention requirements of those systems.

The retention period for data maintained in ATS will not exceed fifteen years, after which time it will be deleted, except as noted below. The retention period for PNR, which is contained only in ATS-P, will be subject to the following further access restrictions: ATS-P users will have general access to PNR for seven years, after which time the PNR data will be moved to dormant, non-operational status. PNR data in dormant status will be retained for eight years and may be accessed only with approval of a senior DHS official designated by the Secretary of Homeland Security 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 law enforcement lookout records, CBP matches to enforcement activities, investigations or cases (i.e., specific and credible threats, and flights, individuals and routes of concern, or other defined sets of circumstances), will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

A NARA Electronic Records Appraisal Questionnaire was completed for Passenger Name Record (PNR) Data in spring 2005. Efforts are underway and ongoing to obtain NARA approval for the remaining data retained in ATS.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

Information in ATS is retained for a period of fifteen years 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 clearer. Passenger records including historical records are essential in assisting CBP Officers with their risk-based screening 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.

The touchstone for data retention is the data's relevance and utility. Accordingly, CBP will regularly review the data maintained in ATS to ensure its continued relevance and usefulness. If no longer relevant and useful, CBP will delete the information.

All risk assessments need to be maintained because the risk assessment 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.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

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

- CBP Office of Field Operations (OFO)

- CBP Office of Intelligence (OI)
- CBP National Targeting Center (NTC)
- CBP Office of International Trade (OT)
- U.S. Immigration and Customs Enforcement (ICE)
- DHS Office of Intelligence and Analysis
- Transportation Security Administration

The information collected through ATS may be shared with component agencies within DHS on a need to know basis consistent with the component's mission. Access to ATS is role-based according to the mission of the component and the user's need to know.

4.2 For each organization, what information is shared and for what purpose?

Authorized users from CBP OFO, OI, and the NTC have full access to all the ATS modules for purposes of enforcing U.S. laws related to the entry into and exit from the United States of persons, cargo, and conveyances. Authorized users from ICE in support of their customs and immigration law enforcement function, TSA in support of their International Pre-screening vetting functions before passenger boarding of an aircraft, and the DHS Office of the Secretary and DHS Office of Intelligence and Analysis in support of their law enforcement and counter-terrorism responsibilities.

Finally, data collected and/or maintained in ATS (including PNR) may be shared with any DHS components or offices that have a need for the information in the performance of their duties under 5 U.S.C. §552a(b)(1) consistent with U.S. law, DHS, and CBP policy, the ATS SORN, and any applicable arrangements or agreements. These purposes may include national security, law enforcement, immigration, intelligence, and other DHS mission-related functions and to provide associated testing, training, management reporting, planning, and analysis.

4.3 How is the information transmitted or disclosed?

Data may be retrieved through authorized users logging in to the CBP network remotely using encryption and passwords to access the ATS web-based interface. Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. Data maintained in ATS may also be shared with other components with a need to know on a case-by-case basis, consistent with U.S. law, DHS and CBP policies, and any applicable arrangements or agreements.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

The key privacy risk concerns the potential number of DHS personnel with access to the system. This risk is mitigated and managed by employing user profiles that define rights and responsibilities concerning a user's access to data contained in the system. The principal method for determining what access rights and system responsibilities a user will have is reference to the user's need-to-know. Need-to-know determinations are covered by internal CBP policies and procedures that relate a user's mission or operational responsibilities to the specific subset of data, contained within ATS, that supports those functions. For example, users at a seaport on the East coast do not have access to current risk assessment data associated with an arriving air traveler at a West coast airport. ATS retains audit logs for all user access. These logs are reviewed to ensure that a user should have no more access than is minimally necessary to perform his or her job. Lastly, users are subject to periodic renewal of their access and regular privacy awareness training to maintain attentiveness to the need for safeguarding and the liabilities for inappropriate use or sharing of ATS protected information.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

For the information maintained in ATS (name, risk assessment, rules applied, and PNR), a limited number of users outside of DHS have access to this information. Only if there is a specific information sharing arrangement permitting the development of an outside agency specific rule sub-set will users from that outside agency be permitted to access and review the name, risk assessment, and rules fired based on the rules developed for the outside agency.

Currently such information sharing agreements exist with the following:

- ATS-Inbound access outside of DHS, for access to information regarding imported commodities, include:
  - U.S. Department of Agriculture (this access includes viewing of specific USDA risk assessments and rule sets)
  - U.S. Food and Drug Administration (FDA) (limited to personnel at the FDA Prior Notice Center)
  - Canada Border Security Agency (CBSA) (See section 5.2 below)
- ATS-Outbound access outside of DHS, for access to information regarding exported commodities, include:
  - U.S. Department of Commerce Bureau of Industry and Security

- The Mexican government, through a Memorandum of Understanding (MOU), may submit queries to CBP seeking verification of Mexican import data by U.S. export data. CBP uses ATS to perform the verification. The verification consists of a yes or no indicator regarding whether or not the two data sets are comparable, that is within or outside of a defined range of standard deviation pertaining to the reported valued of the subject commodity. There is no direct access to ATS by Mexico, nor is there any transfer of personally identifiable information or specific trade data pursuant to this arrangement.

- ATS-P access outside of DHS:

  - Various law enforcement task forces outside of DHS require queries to be run against ATS-P data (for example, the FBI-led Joint Terrorism Task Forces). Generally, these task force groups do not have direct access to ATS-P and must present a request for a query to the CBP representative that supports or is part of the requesting task force.

  - Access to PNR may also be facilitated for various law enforcement and counterterrorism agencies, through the receipt of direct requests and authorized releases.

As a graphical user interface for underlying older existing systems, users outside of DHS use ATS as an easier means of accessing these older existing systems. User access is tightly controlled and users may only access the source data consistent with their user roles in the underlying systems. In some instances users have less access through ATS then if they had direct access to the underlying system. Agencies with this type of access include:

- Department of Justice (Federal Bureau of Investigation)

- Department of State (Diplomatic Security)

5.2 What information is shared and for what purpose?

Data obtained from other systems (*e.g.*, ACE, ACS, AES, TECS, APIS, and NCIC) is used to identify cargo, conveyances and travelers at high risk for involvement in terrorist activities or for other statutory violations, such as drug smuggling, alien smuggling, counterfeiting, and intellectual property rights infringement.

USDA users are supported by rule sets specific to the USDA for enforcement of compliance with meat and poultry inspection regulations and other perishable commodity restrictions. USDA users can view the risk assessment and rule history for the USDA specific rule sets only. For all other rule sets, USDA users can view the source data, but may not view the risk assessment.

For all other ATS users outside of CBP, users may view the source data, but may not view the risk assessment. Access to ATS modules and underlying data, as previously stated, is determined by user profiles assigning a particular user rights and responsibilities dependent upon his or her operational and mission functions and authority.

Access to ATS-L and the DMV data for U.S. plated vehicles that it uses is limited to CBP Officers. No other use or dissemination of DMV data is performed.

Canada is currently the only foreign country that accesses data directly using ATS. CBSA users can only view Canadian data provided by Canada. Other countries may, through ATS-I, be permitted to use ATS, but they will likewise be limited to viewing their own data and the related risk assessment and rules applied, if expressly stated within the terms of their particular arrangement.

5.3 How is the information transmitted or disclosed?

For facilitated disclosure, various users outside of DHS must present a request for a query to the CBP representative that supports or is part of the requesting user, task force, agency, etc. Upon CBP approval of the specific request for access, access may be provided either electronically or by hard copy print out.

ATS users access data using the ATS user interface. Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. Data is retrieved through authorized users logging in to the CBP network remotely using encryption and passwords to access the ATS web-based interface.

Access for users outside of DHS is limited to source data only (the access employs ATS as an interface to the ATS image of the underlying database).

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared through the system, and does the agreement reflect the scope of the information currently shared?

Yes, there are agreements in place to share information from ATS. Each agreement defines the nature of access to ATS, including specific modules and scope of information subject to the sharing arrangement. In defining the sharing arrangement, the agreements also set forth the terms and conditions of access to information and the limitations upon the use and redissemination of the information. As an example and as previously noted, the Mexican government is an indirect beneficiary of ATS-Outbound data and is permitted to submit a request for a query to CBP in accordance with an agreement (Memorandum of Understanding, MOU[6]) between CBP and the Mexican government. If CBP approves the request for query, a response is forwarded using secure electronic messaging. (See section 5.1 above.)

[6] CBP has the authority to provide information to foreign customs and law enforcement agencies pursuant to Title 19, United States Code, Section 1628, and more specifically with respect to Mexico's Customs General Administration, as provided for under to the Agreement between the Government of the United States of America and the Government of the United Mexican States Regarding Mutual Assistance Between their Customs Administrations (CMAA), dated June 20, 2000. This MOU is subject to the implementing guidelines contained within the CMAA.

5.5 How is the shared information secured by the recipient?

The terms and conditions within agreements permitting access to ATS set forth the requirements that external users of ATS must meet in order to obtain and maintain access. Generally, CBP's requirements for external users dictate that the external user employ the same or similar security and safeguarding precautions as employed by CBP. 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 Mandatory Access Control, which is based on a demonstrated "need to know."

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

CBP requires all external users of ATS information to receive the same training as CBP users regarding the safeguarding, security, and privacy concerns relating to information stored in the ATS database. This means that users are subject to periodic recertification of their access (typically every six months), that they receive initial functional training related to their particular access and role, and that they are required to complete and pass a system based privacy awareness course (initially before access, and every year, thereafter).

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

When sharing information with external agencies, similar risks are posed as those arising with respect to internal sharing with DHS. To this extent the agreements with external agencies require similar measures to be employed relating to security, privacy, and safeguarding of information.

Separately, an additional risk is posed by the potential for further dissemination of information by the external agency to a third agency. Again, the terms and conditions of the agreement, which provides for access by an external agency, address and mitigate this risk, in the confidentiality section of each agreement, by requiring any further dissemination of shared data outside of the receiving agency to be subject to prior authorization by CBP. Lastly, CBP emphasizes that, within each agreement, each external user is provided with training, as outlined in paragraph 5.6, designed to ensure that data that is accessed through ATS is safeguarded and secured in an appropriate manner, consistent with applicable laws and policies.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

ATS does not collect any information directly from individuals. ATS does collect and maintain passenger name record (PNR) data derived from air carrier reservation/departure control systems, as indicated in the SORN for ATS originally published on November 2, 2006 at 71 FR 64543 and discussed above at paragraph 1.1 and as revised and published in the Federal Register on August 6, 2007 at 72 FR 43650.

In cases where an individual has a concern about the information collected during an interaction with a CBP officer, the CBP officer may provide the individual with a copy of the CBP Screening Fact Sheet (See Appendix), which provides both 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.

Most of the information that ATS uses is collected from government data sources. Notice was provided for these sources under the applicable source systems of records and privacy impact assessments, as well as through the publication of the laws and regulations authorizing the collection of such information. For information collected from the carriers, template privacy statements were drafted and provided to the carriers for inclusion in their privacy statements and are encouraged to include discussion in their privacy statements.

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

6.2 Do individuals have an opportunity and/or right to decline to provide information?

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 goods and merchandise in the U.S. are required to provide certain information to allow CBP to determine whether the goods/merchandise may enter the U.S. ATS does not require individuals to provide information beyond that authorized by law. This is also the case for travelers, conveyances and cargo exiting the United States. This information is captured by the source systems (*e.g.*, ATS, ACS, 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.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

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, export, ship, or mail any goods/merchandise to, from, or through the United States restrictions on CBP use and sharing of accessed information are limited to legal requirements set forth in the Privacy Act, Trade Secrets Act, and the uses published in the SORN. Consent to store or use this information must be done in accordance with the above legal requirements.

ATS does not directly collect information from individuals. Opportunities for individuals to consent to particular uses of information would be addressed using the process defined by the source systems. All information collected by these systems is mandated by law.

Many air carriers have provided their own notice to customers concerning these requirements. Template privacy statements with information about PNR were provided to carriers and carriers are encouraged to include discussion in their privacy statements.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

There is a risk that the individual may not know that the information is being used by ATS in the ways described. As such, CBP has published the System of Records Notice and this PIA to increase transparency of its operations. Additionally, it has drafted language for commercial carriers to include in their privacy statements so as to provide further transparency and CBP encourages inclusion in the carriers' privacy statements.

Section 7.0 Individual Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures which allow individuals to gain access to their own information?

DHS allows persons, including foreign nationals, to seek access under the Privacy Act to information maintained in ATS, specifically PNR data submitted to ATS-P. Requests for access to personally identifiable information contained in ATS-P, that was provided regarding the requestor,

by the requestor or by someone else on behalf of the requestor may be submitted to the FOIA/PA Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5-C, 1300 Pennsylvania Avenue, NW, Washington, DC 20229 (phone: (202)344-1850 and fax: (202)344-2791).

Requests should conform to the requirements of 6 CFR Part 5, which provides the rules for requesting access to Privacy Act records maintained by DHS. The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury.

CBP notes that ATS is a decision support tool that compares various databases, but does not actively collect the information in those respective databases except for PNR. When an individual is seeking redress for other information analyzed in ATS, such redress is properly accomplished by referring to the databases that directly collect that information.

If individuals are uncertain what agency handles the information, they may seek redress through the DHS Traveler Redress Program ("TRIP") (See 72 Fed. Reg. 2294, dated January 18, 2007). Individuals who believe they have been improperly denied entry, refused boarding for transportation, or identified for additional screening by CBP may submit a redress request through the TRIP. TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs – like airports and train stations or crossing U.S. borders. Through TRIP, a traveler can request correction of erroneous PNR data stored in ATS and other data stored in other DHS databases through one application. Redress requests should be sent to: DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip.

To address situations where a traveler has the same or similar name as to someone on a watchlist, CBP has developed procedures to identify these travelers as such.

Specifically, a system upgrade was developed in TECS in February 2006 that benefits anti-terrorism security measures, as well as the customs and immigration process for international travelers. The enhancement, which is virtually transparent to travelers, strives to alleviate additional screening procedures for passengers who have been misidentified due to the same or similar biographical information as watch-listed individuals.

The upgrade, which is essentially an annotation in CBP's TECS database, allows CBP officers at ports of entry to eliminate inspections on subsequent trips in cases where travelers' names, birthdates or other biographical information matches those of high-risk individuals once CBP has verified that the individual is not the person of interest. No action is needed from the passenger. There is no additional data collected on the passenger beyond what is normally collected during a secondary type examination. TECS will suppress the records from appearing on subsequent encounters with the traveler.

Procedures for individuals to gain access to data maintained in source systems that provide data used by ATS would be covered by the respective SORNs for the source systems. In addition,

the Freedom of Information Act (FOIA) (5 U.S.C. 552) provides a means of access to information, including PNR data, for all persons, irrespective of the individual's status under the Privacy Act.

With respect to data for which ATS is the actual source system (*e.g.*, PNR), the ATS SORN is published at 72, Federal Register XX, published June XX, 2007. FOIA requests for access to information for which ATS is the source system may be directed to CBP in the manner prescribed by regulations at Title 19, Code of Federal Regulations, Part 103.

With respect to the data that ATS creates, i.e., the risk assessment for an individual, the risk assessment is for official law enforcement use only and is not communicated outside of CBP staff, nor is it subject to access under the Privacy Act. ATS is a system that supports CBP law enforcement activities, as such an individual might not be aware of the reason additional scrutiny is taking place, nor should he or she be aware of the reason for additional scrutiny as this may compromise the means and methods of how CBP came to require further scrutiny. Additional screening may occur because of a heightened risk assessment, or because of other concerns by the CBP officer, or on a random basis. If a reviewing officer determines that a person is not a match to a record or the record is determined to not be accurate, CBP has a policy in place which permits the officer to promptly initiate corrective action with regard to that record to avoid that person being identified for examination during future entry or exit processing based on that erroneous information.

7.2 What are the procedures for correcting erroneous information?

Individuals may seek redress and/or contest a record through two different means. Both will be handled in the same fashion. If the individual is aware the information is specifically handled by CBP, requests may be sent directly to CBP at the FOIA/PA Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5-C, 1300 Pennsylvania Avenue, NW, Washington, DC 20229 (phone: (202) 344-1850 and fax: (202) 344-2791). If the individual is uncertain what agency is responsible for maintaining the information, redress requests may be sent to DHS TRIP at DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip.

CBP has created a FOIA/PA Unit in its Office of Field Operations to provide redress with respect to inaccurate information collected or maintained by its electronic systems, which include ATS, TECS, ACE, ACS, and APIS). Inquiries to the FOIA/PA Unit should be addressed to: FOIA/PA Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5C, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229. Individuals making inquiries should provide sufficient information to identify the record at issue.

DMV data to support ATS-L is obtained from a government source, NLETS. If problems with the DMV data are identified through the redress process, the problem would be communicated to NLETS. Upon request, CBP officers will provide the Screening fact sheet that provides information on appropriate redress. The redress process includes the ability to correct data in the source systems including TECS.

ATS incorporates the procedures of the source systems with respect to error correction. Once any updates or corrections are made, they are transmitted to ATS. Corrected data becomes available to ATS almost immediately after the correction is entered to the source system. ATS monitors source systems for changes to the source system databases. Continuous source system updates occur in real-time, from ACS, AES, and TECS. When corrections are made to data in source systems, ATS reflects these updates to data, accordingly.

7.3 How are individuals notified of the procedures for correcting their information?

Upon request, CBP officers will provide the CBP Screening fact sheet that provides information on appropriate redress. The redress procedure provides the ability to correct data in the source systems including TECS. Publication of the source system SORNs also provides information on accessing and amending information collected through those systems. There is no procedure to correct the risk assessment and associated rules stored in ATS as the assessment is based on the underlying data and will change when the data from source system(s) is amended.

7.4 If no redress is provided, are alternatives available?

Redress is provided.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

As set forth in the ATS SORN (71 FR 64543, November 2, 2006, as revised and published in the Federal Register on August 6, 2007 at 72 FR 43650), CBP provides limited access and amendment in ATS to PNR data obtained from or about a person. In doing so, CBP seeks to permit all persons to be able to obtain copies of the PNR data that they or their agent (*e.g.*, travel agent, air carrier, booking agent, *etc.*) submitted on their behalf as part of the process of engaging air travel. No exemption shall be asserted regarding PNR data about the requester, obtained from either the requester or by a booking agent, brokers, or another person on the requester's behalf. This information, upon request, may be provided to the requester in the form in which it was collected from the respective carrier, but may not include certain business confidential information of the air carrier that is also contained in the record.

Pursuant to 6 CFR Part 5, Appendix C, certain records and information in this system are exempt from 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) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2) and (k)(2)). With respect to ATS-P module, exempt records are the risk assessment analyses and business confidential information received in the PNR from the air and vessel carriers. For other ATS modules the only information maintained in ATS is the risk assessment analyses and a pointer to the data from the source system of records.

With regard to personally identifiable information in ATS that was obtained from another system, access under the Privacy Act to that information is covered by the system of records notice for the respective system (*e.g.*, ACE, ACS, TECS, or APIS) As noted above in paragraph 7.1, individuals may also seek access to information collected in ATS or originating from a government source system pursuant to the FOIA, and as a matter of CBP policy, redress may also be requested in the manner described above in paragraph 7.2.

Section 8.0 Technical Access and Security

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

8.1 Which user group(s) will have access to the system?

Each user groups' access to the system is defined by the specific profile created for that group. Group profiles are intended to limit access by reference to the common rights and mission responsibilities of users within the group. 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. User access to data is based on a demonstrated need-to-know by a user.

8.2 Will contractors to DHS have access to the system?

Yes, subject to the same background, training, need-to-know, and confidentiality requirements as employees.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes, ATS user access is restricted in the form of Mandatory Access Controls 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 with the ATS Security Desk procedures referenced in the section above and roles are assigned only after supervisor request, process owner approval, and appropriate security checks have been confirmed.

8.4 What procedures are in place to determine which users may access the system and are they documented?

Initial requests for grants to the system are routed from the user through their supervisor to the specific CBP Process Owners. Need-to-know determinations are made at both the supervisor and process owner level. If validated, the request is passed on to the Security Help Desk. Once received, 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, on a periodic basis access is reviewed by the process owner, on a periodic basis, to ensure that only appropriate individuals have access to the system.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

ATS User roles are highly restricted and audited.

Application access is restricted in the form of Mandatory Access Control, 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. Data is retrieved through authorized users logging in to the CBP network remotely using encryption and passwords to access to ATS web-based interface.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

On a periodic basis access is reviewed by the process owner to ensure that only appropriate individuals have access to the system. Additionally, CBP's Office of Internal Affairs conducts periodic reviews of the ATS system in order to ensure that the system is being accessed and used in accordance with documented DHS and CBP policies.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

The CBP process owners and all system users are required to complete annual training in privacy awareness. If an individual does not take training, he/she will lose access to all computer systems, which are integral to his/her duties as a CBP Officer.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

ATS underwent the Certification and Accreditation (C&A) process in accordance with DHS and CBP policy, which complies with these Federal statutes, policies, and guidelines, and was certified and accredited on June 16, 2005, for a three year period.

A Security Risk Assessment was completed on March 28, 2006 in compliance with FISMA, OMB policy and NIST guidance.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Privacy risks identified with respect to access and security were in appropriate use and access of the information. These risks are mitigated through training, background investigations, internal system audit controls, CBP Code of Conduct and Disciplinary system, and the practice of least privileged access.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

ATS was built from the ground up.

The data collected through ATS is maintained using existing data models in the source systems of records.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Integrity, privacy, and security are analyzed as part of the decisions made for ATS in accordance with CBP security and privacy policy from the inception of ATS, as demonstrated by the successful transition through the systems development lifecycle (SDLC), certification and accreditation, and investment management processes. Particular areas that were identified as needing to be addressed during the development included: use of accurate data, system access controls, and audit capabilities to ensure appropriate use of the system.

9.3 What design choices were made to enhance privacy?

The system was developed so that the rules are building risk assessments based on the most accurate information available in the source systems. This improves the data integrity of the system. User access controls were developed in order to ensure that only the minimum number of individuals with a need to know the information are provided access to the information. Audit provisions in conjunction with policies and procedures were also put in place to ensure that the system is properly used by CBP officers.

The system is designed to provide the following privacy protections:

- Equitable risk assessment:
    - ATS provides equitable treatment for all individuals. Equitable risk assessment is provided because ATS uses the same risk assessment process for everybody (using a defined targeting methodology for a given period at a specific port).

- ATS applies the same methodology to all individuals to preclude any possibility of disparate treatment of individuals or groups. ATS is consistent in its evaluation of risk associated with individuals and is used to support the overall CBP law enforcement mission.

- ATS supports a national targeting policy that is established at the National Targeting Center. CBP policies regarding inspections and responding to potential terrorists and other criminals seeking entry into the United States are documented in various CBP Directives and individuals with access to the system are trained on the appropriate use of the information.

- CBP's secure encrypted network:

  - ATS security processes, procedures, and infrastructure provide protection of data, including data about individuals that is stored in ATS databases.

  - Encryption and authentication are the technical tools used to protect all ATS data, including data about individuals.

- ATS's role as a decision support tool for CBP officers:

  - As a decision support system, ATS is employed to support but not replace the decision-making responsibility of CBP officers and analysts. The information accessed in ATS is not the conclusion about whether or not to act but merely part of the basis upon which a CBP officer will make his or her decision. Human intervention, professionalism, and training all serve to mitigate the potential privacy threat posed by data comparisons made outside of an operational context.

In order to enhance privacy and transparency, a separate and distinct System of Records under the Privacy Act was published to address both the risk assessments derived using ATS, the rules applied, as well as other information for which ATS is considered the actual source system (i.e, PNR). The SORN for ATS was published in the Federal Register on August 6, 2007 at 72 FR 43650.

Additionally, access to the assessment and related rules is limited to a small number of CBP officers who have gone through extensive training on the appropriate use of the information and CBP targeting policies. These CBP officers are trained to review the risk assessments and the underlying information to identify cargo and individuals that truly pose a risk to law enforcement.

Conclusion

ATS is a decision support tool used by CBP officers to identify individuals, cargo and conveyances that may require additional scrutiny based on observations related to data describing those individuals.

The ATS system supports CBP officers in identifying individuals or cargo that may be a risk to U.S. law enforcement, but it does not replace their judgment in determining whether the individual or goods/merchandise, as applicable, should be allowed into the country.

ATS offers equitable risk assessment using a secure encrypted network; however, it is the policies and procedures and laws that govern the inspection and other law enforcement processes that ultimately protect individual privacy rights. The professionalism applied by CBP officers serves to further protect individual privacy rights.

Appendix A: Detailed Description of Information Sources Being Compiled

The information ATS uses is described by module and is presented in the following format.

- Nature, Source

ATS- Inbound: Collects information about Importers and cargo and conveyances used to import cargo to the United States from destinations outside its borders. Information regarding individuals, such as importers, that is collected in connection with items identified below, include, but are not limited to,

- Sea/Rail Manifests (bills of lading), Automated Manifest System (AMS)
- Cargo Selectivity Entries, Automated Broker Interface (ABI)
- Entry Summary Entries, ABI
- Air Manifest (bills of lading), AMS-Air
- Express Consignment Services (bills of lading)
- CCRA Manifest (bills of ladings), Canada Customs and Revenue (CCRA)
- CAFÉ, QP Manifest Inbound (bills of lading), AMS
- Truck Manifest, Automated Commercial Environment (ACE)
- Inbound Data (bills of lading), AMS
- Food and Drug Administration (FDA) Entries/Prior Notice (PN), Automated Commercial System (ACS)
- Census Import Data, Department of Commerce

ATS-Outbound: Collects information about exporters and cargo and conveyances used to transport cargo from the United States to destinations outside its borders.

- Shippers Export Declarations, Automated Export System (AES)
- Export Manifest Data, AES
- Export Air Way Bills of Lading
- Census Export Data, Department of Commerce

ATS-L: Collects information about vehicles and persons crossing land border locations. This data includes license plate numbers for vehicles entering the United States, vehicle and registered owner data (derived from state DMV records).

- Publicly Available State DMV Data
- Border Crossing, TECS
- Seizures, TECS

ATS-P: Collects information about travelers entering the United States from destinations outside its borders. This data includes passenger manifests, immigration control information and PNR information (for which ATS is the source system).

- Advance Passenger Information System (APIS)
- Border Crossing, TECS
- Land Border Crossing, TECS
- I-94, TECS[7]
- Personal Search, TECS
- Secondary Referrals, TECS
- Secondary Referrals/Land, TECS
- Secondary Referrals/CBP/ICE, TECS
- Seized Property, TECS
- Seized Vehicle, TECS
- USVISIT, TECS[8]
- NCIC III, TECS
- Air Craft Arrivals, ACS
- PNR (Approximately 100 airlines), Airline Reservations System data collected in ATS
- Visa, TECS
- Enforcement Subjects: Person, TECS
- Enforcement Subjects: Business, TECS
- Enforcement Subjects: Address, TECS

[7] ATS receives I-94 data via TECS. TECS receives I-94 data directly from the source ICE system.
[8] ATS receives USVISIT data via TECS. TECS receives US VISIT data directly from USVISIT.

ATS-TAP: Collates information derived from ATS- Outbound and ATS-Inbound.

ATS also uses watchlisted data and data regarding other high risk parties:

- Debarred Parties, Dept of State ODTC
- Nuclear Proliferation, Dept of Commerce BXA
- Specially Designated Parties, Dept of Treasury OFAC

Appendix B Types of Information included in PNR

PNR may include some combination of 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, etc)
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
9. Travel itinerary for specific PNR
10. Travel agency/travel agent
11. Code share information
12. Split/divided information
13. Travel status of passenger (including confirmations and check-in status) and relevant travel history
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. Open text fields
18. Any collected APIS information
19. All historical changes to the PNR listed in numbers 1 to 18

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.

*****Not all carriers collect PNR and of those that do collect this data, not all collect the same sets of PNR data.

Responsible Officials

Laurence Castelli, Chief, Privacy Act Policy and Procedures Branch, Office of Regulations and Rulings, CBP, (202) 572-8790.

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security