BILLING CODE: 4410-10

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

DHS-2007-0042

Privacy Act of 1974; U.S. Customs and Border Protection, Automated Targeting System, System of Records

AGENCY: Privacy Office; Department of Homeland Security

ACTION: Notice of Privacy Act System of Records.

SUMMARY: This document is a new System of Records Notice (SORN) for the Automated Targeting System (ATS) and is subject to the Privacy Act of 1974, as amended. ATS is an enforcement screening tool consisting of six separate components, all of which rely substantially on information in the Treasury Enforcement Communications System (TECS). ATS historically was covered by the SORN for TECS. The Department of Homeland Security, U.S. Customs and Border Protection (CBP) published a separate SORN for ATS in the Federal Register on November 2, 2006. This SORN did not describe any new collection of information and was intended solely to provide increased notice and transparency to the public about ATS. Based on comments received in response to the November 2, 2006 notice, CBP issues this revised SORN, which responds to those comments, makes certain amendments with regard to the retention period and access provisions of the prior notice, and provides further notice and transparency to the public about the functionality of ATS.

TECS is an overarching law enforcement information collection, risk assessment, and information sharing environment. It is also a repository for law enforcement and investigative information. TECS is comprised of several modules that collect, maintain, and evaluate screening data, conduct targeting, and make information available to appropriate officers of the U.S. government. ATS is one of those modules. It is a decision support tool that compares traveler, cargo, and conveyance information against intelligence and other enforcement data by incorporating risk-based targeting scenarios and assessments. As such, ATS allows DHS officers charged with enforcing U.S. law and preventing terrorism and other crimes to effectively and efficiently manage information collected when travelers or goods seek to enter, exit, or transit through the United States.

Within ATS there are six separate and distinct components that perform screening of inbound and outbound cargo, conveyances, or travelers. These modules compare information received against CBP's law enforcement databases, the Federal Bureau of Investigation Terrorist Screening Center's Terrorist Screening Database (TSDB), information on outstanding wants or warrants, information from other government agencies regarding high-risk parties, and risk-based rules developed by analysts using law enforcement data, intelligence, and past case experience. The modules also facilitate analysis of the screening results of these comparisons. In the case of cargo and conveyances, this screening results in a risk assessment score. In the case of travelers, however, it does not result in a risk assessment score.

DATES: The new system of records will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Laurence E. Castelli (202-572-8790), Chief, Privacy Act Policy and Procedures Branch, U.S. Customs and Border Protection, Office of International Trade, Mint Annex, 1300 Pennsylvania Ave., NW, Washington, DC 20229. For privacy issues please contact: Hugo Teufel III (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

BACKGROUND

The System

The priority mission of CBP is to prevent terrorists and terrorist weapons from entering the country while facilitating legitimate travel and trade. ATS uses CBP's law enforcement databases, the Federal Bureau of Investigation Terrorist Screening Center's Terrorist Screening Database (TSDB), information on outstanding wants or warrants, information from other government agencies regarding high-risk parties, 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. These rules are based on investigatory and law enforcement data, intelligence, and past case experience. Historically, the SORN for

the Treasury Enforcement Communications System (TECS) covered ATS. As part of DHS's updating of its system of records notices and in an effort to provide more detailed information to the traveling public and trade community, DHS has decided to notice ATS as a separate Privacy Act system of records, giving greater visibility into its targeting and screening efforts.

TECS is an overarching law enforcement information collection, risk assessment, and information sharing environment. It is also a repository for law enforcement and investigative information. TECS is comprised of several modules that collect, maintain, and evaluate screening data, conduct targeting analysis, and make information available to appropriate officers of the U.S. government. ATS is one of those modules. It is a decision-support tool that compares traveler, cargo, and conveyance information against intelligence and other enforcement data by incorporating risk-based targeting scenarios and assessments. As such, ATS allows DHS officers charged with enforcing U.S. law and preventing terrorism and other crime to effectively and efficiently manage information collected when travelers or goods seek to enter, exit, or transit through the United States. Within ATS there are six separate and distinct components that perform screening of inbound and outbound cargo, conveyances, or travelers by comparing information received against CBP's law enforcement databases, the Federal Bureau of Investigation Terrorist Screening Center's Terrorist Screening Database (TSDB), information on outstanding wants or warrants, information from other government agencies regarding high-risk parties, and risk-based rules developed by analysts based on law enforcement data, intelligence, and past case experience. The modules also facilitate analysis of the screening results of these comparisons.

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. Today, ATS includes the following separate components: ATS-N, for screening inbound or imported cargo; ATS-AT, for outbound or exported cargo; ATS-L, for screening private passenger vehicles crossing at land border ports of entry using license plate data; ATS-I, for cooperating with international customs partners in shared cargo screening and supply chain security; ATS-TAP, for assisting tactical units in identifying anomalous trade activity and performing trend analysis; and ATS-P, for screening travelers and conveyances entering the United States in the air, sea, and rail environments. The Privacy Impact Assessment (PIA)—which DHS will publish on its web site (www.dhs.gov/privacy) concurrently with the publication of the SORN in the Federal Register—provides a full discussion of the functional capabilities of ATS and its components. It is worth clarifying here, 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.

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-P's screening relies upon information from the following databases: TECS, the Advanced Passenger Information System (APIS), the Non Immigrant Information System (NIIS), the Suspect and Violator Indices (SAVI), and the Department of State visa databases, as well as the PNR information that it maintains. As stated 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 by analysts based upon 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. 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. In lieu of manual reviews of traveler information and intensive interviews with every traveler arriving in or departing from the United States, ATS-P allows CBP personnel to focus their efforts on potentially high-risk passengers.

The Legal Requirements

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates personally identifiable information. The Privacy Act applies to information that is maintained in a "system of records." A system of records is a group of any records under the control of an agency from which information is retrieved by the name of the

individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. ATS involves the collection and creation of information that is maintained in a system of records. ATS also stores information on individuals other than U.S. citizens and lawful permanent residents (LPRs). As a matter of administrative policy, where the PII of individuals other than U.S. citizens and LPRs is held in mixed systems (i.e., a system also including U.S. citizen or LPR), DHS will accord such PII the fair information principles set forth the Privacy Act.

The Privacy Act requires each agency to publish in the Federal Register a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system to make agency recordkeeping practices transparent, to notify individuals regarding the uses to which personally identifiable information is put, to assist the individual to more easily find such files within the agency, and to inform the public if any applicable Privacy Act exemptions will be claimed for the system.

Access to information in ATS may be provided. However, as discussed further later in this notice, certain records within ATS are exempt from certain provisions of the Privacy Act (specifically, those provisions contained at 5 U.S.C. 552a (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (5), and (8); (f), and (g)) pursuant to 5 U.S.C. 552a(j)(2) and (k)(2)). Notwithstanding the listed exemptions for the system, individuals, regardless of their citizenship, may make a written request to review and access personal data provided by and regarding the requester, or provided by a booking agent, brokers, or other person on the requester's behalf, that is collected by CBP and

contained in the PNR database stored in the ATS-P, and correct any inaccuracies. Data collected and maintained from air carriers as PNR are listed later in this notice in the "Categories of Records in the System" section of this notice; the listed categories are not specific data elements because each carrier varies its configuration of PNR to meet its business needs. In an effort to provide some consistency in the description of PNR data for the traveling public, CBP has categorized the various data that generally comprise PNR for air carriers into the 19 categories listed in the SORN. The PNR data, 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, such as use and application of frequent flier miles, internal annotations to the air fare, etc.

To obtain access to a requestor's own PNR, contact the FOIA/PA Branch, 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). Additionally, regardless of their citizenship, individuals who believe they have been erroneously denied entry, refused boarding for transportation, or identified for additional screening by CBP may submit a redress request through DHS Traveler Redress Inquiry Program ("TRIP"). (S*ee* 72 Fed. Reg. 2294, January 18, 2007). For further information on the Automated Targeting System and the redress options, please see the accompanying Privacy Impact Assessment for the Automated Targeting System at www.dhs.gov/privacy under "Privacy Impact Assessment." Redress requests should be sent to: Systems Manager, DHS TRIP, U.S. Department of Homeland Security, Washington, DC.

DHS is hereby publishing a description of the system of records referred to as the Automated Targeting System. In accordance with 5 U.S.C. 552a(r), a report concerning this record system has been sent to the Office of Management and Budget and to the Congress.

DISCUSSION OF REVISIONS ARISING FROM PUBLIC COMMENTS

On November 2, 2006, CBP issued a Privacy Act System of Records Notice for ATS (71 FR 64543). DHS received a number of comments and decided to extend the comment period until December 29, 2006, by Federal Register Notice dated December 8, 2006 (71 FR 71182). A total of 641 comments were received in response to the SORN. After considering these comments, CBP has made the following substantive changes to the previously issued SORN. First, the general retention period for data maintained in ATS is reduced from 40 years to a total of 15 years. CBP has determined that it can continue to uncover and use information relating to terrorism and other serious crimes within this shorter retention period.

This retention period is consistent with the retention period currently contained in international agreements entered into by the Department. Furthermore, CBP has limited access to the last eight years of the retention period for PNR data to those users who first obtain supervisory approval to access the archive where the data is maintained. CBP, however, has created an exception to this general retention period such that PNR data, as well as any other data that may be stored in ATS, which becomes associated with active law enforcement activities, and/or investigations or cases (*i.e.*, specific and credible threats; flights, individuals, and routes of concern; or other defined sets of circumstances)

will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

Second, persons whose PNR data has been collected and maintained in ATS-P will have administrative access to that data under the Privacy Act. This data will be available in the same format that it was obtained by CBP (with the exception of business confidential information that may be contained in the record). These individuals will also be able to seek to correct factual inaccuracies contained in their PNR data, as it is maintained by CBP. CBP believes that permitting persons to access and to seek to amend their PNR data will reduce the incidence of potential misidentifications and improve the accuracy of the data within ATS-P.

Third, CBP has added the following category to the categories of persons from whom information is obtained: "Persons who serve as booking agents." Several commenters correctly noted that many in the traveling public utilize the services of booking agents and that booking agents' identities are included in itinerary information.

Fourth, to be consistent with the forthcoming SORN for the Advanced Passenger Information System (APIS), CBP has amended category A to include persons whose international itineraries cause their flight to stop in the United States, either to refuel or to permit a transfer, and crewmembers on flights that overfly or transit through U.S. airspace.

Fifth, as stated above, CBP has clarified the categories of PNR data collected and maintained in ATS-P to more accurately reflect the type of data collected from air carriers. Consistent with its particular business needs, each air carrier determines the specific configuration of data elements that ultimately constitute PNR. By providing

increased notice of the types of data that may be contained within PNR, CBP seeks to provide the public with a greater understanding of the personal information being maintained in ATS-P. Examples of these categories of PNR, as listed below under "Categories of Records" include: name, date of issuance ticket, date(s) of travel, PNR locator number, payment information, such as credit card information, and travel agent or travel agency that may have made the reservations for the individual.

Lastly, two of the routine uses included in the earlier version of the SORN—those pertaining to using ATS in background checks—are removed. This is necessary because the revised SORN contains a more narrow definition of the purposes for which certain data—specifically, PNR data maintained in ATS-P—will be used. The deleted routine uses did not fit within the scope of these purposes.

This discussion of comments addresses revisions made to the SORN published on November 2, 2006. The full comments received address additional issues, such as mission creep, potential economic impact, appropriate applicability of the Privacy Act, constitutionality, and information quality. For a discussion of the full comments received from the November 2, 2006, publication and DHS' response, please see "Discussion of Public Comments Received on the Automated Targeting System Privacy Act System of Records Notice" on the DHS website at www.dhs.gov/privacy

SYSTEM NAME:

Automated Targeting System (ATS) – CBP

SYSTEM LOCATION:

This computer database is located at the CBP National Data Center in Washington, D.C. Computer terminals are located at customhouses, border ports of entry, airport inspection

facilities under the jurisdiction of DHS, and other locations at which DHS authorized personnel may be posted to facilitate DHS's mission. Terminals may also be located at appropriate facilities for other participating government agencies pursuant to agreement.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM.

ATS includes the following separate components: ATS-N, for screening inbound or imported cargo; ATS-AT, for outbound or exported cargo; ATS-L, for screening private passenger vehicles crossing at land border ports of entry by license plate data; ATS-I, for cooperating with international customs partners in shared cargo screening and supply chain security; ATS-TAP, for assisting tactical units in identifying anomalous trade activity and performing trend analysis; and ATS-P, for screening travelers and conveyances entering the United States in the air, sea and rail environments. Collectively, these components handle information relating to the following individuals:

A. Persons seeking to enter, exit, or transit through the United States by land, air, or sea. This includes passengers who arrive and depart the United States by air or sea, including those in transit through the United States on route to a foreign destination and crew members who arrive and depart the United States by air or sea, including those in transit through the United States on route to a foreign destination, and crew members on aircraft that over fly the United States.

B. Persons who engage in any form of trade or other commercial transaction related to the importation or exportation of merchandise.

C. Persons who are employed in any capacity related to the transit of merchandise intended to cross the United States border.

D. Persons who serve as operators, crew, or passengers on any vessel, vehicle, aircraft, train, or other conveyance that arrives in or departs the United States.

E. Persons who serve as booking agents, brokers, or other persons who provide information on behalf of persons seeking to enter, exit, or transit through the United States.

CATEGORIES OF RECORDS IN THE SYSTEM:

ATS uses CBP's law enforcement databases, the Federal Bureau of Investigation Terrorist Screening Center's Terrorist Screening Database (TSDB), information on outstanding wants or warrants, information from other government agencies regarding high-risk parties, and risk-based rules developed by analysts to assess and identify high-risk cargo, conveyances, or travelers that should be subject to further scrutiny or examination. ATS maintains these assessments together with a record of which rules were used to develop the assessment. With the exception of PNR information, discussed below, ATS maintains a pointer or reference to the underlying records from other systems that resulted in a particular assessment.

ATS-P, a component of ATS, maintains the PNR information obtained from commercial air carriers and uses that information to assess whether there is a risk associated with any travelers seeking to enter, exit, or pass through the United States. PNR may include some combination of these following categories 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 (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 air carriers maintain the same sets of information for PNR, and a particular individual's PNR likely will not include information for all possible categories.

In addition, PNR does not routinely include information that could directly indicate the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, or sex life of the individual. To the extent PNR does include terms that reveal such personal matters, DHS employs an automated system that filters certain of these terms and only uses this information in exceptional circumstances.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

19 U.S.C. 482, 1461, 1496, and 1581-82, 8 U.S.C 1357, Title VII of Public Law 104-208, 49 U.S.C. 44909, and the "Security and Accountability for Every Port Act of 2006" (SAFE Port Act) (P.L. 109-347).

Purposes for PNR in ATS-P:

(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.

Purposes of ATS (except PNR in ATS-P):

In addition to those purposes listed above for PNR in ATS-P:

(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.

Routine uses of records maintained in the various components of ATS, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3). DHS only discloses information to those authorities who have a legal purpose to use the data, intend to use the information consistent with the purpose for which CBP collects it or for another legally required function, such as GAO oversight and ongoing IT maintenance, and has sufficient capability to protect and safeguard it. Under these limits, data may be disclosed as a routine use in the following manner:

A. To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where CBP believes the information would assist enforcement of applicable civil or criminal laws;

B. To Federal and foreign government intelligence or counterterrorism agencies or components where CBP becomes aware of an indication of a threat or potential threat to national or international security, or where such use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure;

C. To an organization or individual in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, or where the information is relevant to the protection of life, property, or other vital interests of a data subject and such disclosure is proper and consistent with the official duties of the person making the disclosure;

D. To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk;

E. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations, or in response to a subpoena, or in connection with criminal law proceedings;

F. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is

appropriate in the proper performance of the official duties of the officer making the disclosure.

G. To an agency, organization, or individual for the purposes of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function;

H. To a Congressional office, for the record of an individual in response to an inquiry from that Congressional office made at the request of the individual to whom the record pertains;

I. To contractors, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government, when necessary to accomplish an agency function related to this system of records, in compliance with the Privacy Act of 1974, as amended;

J. To the U.S. Department of Justice (including U.S. Attorney offices) or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation: (a) DHS, or (b) any employee of DHS in his/her official capacity, or (c) any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent said employee, or (d) the United States or any agency thereof;

K. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. Sections 2904 and 2906;

L. To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations where CBP is aware of a need to utilize relevant data for purposes of testing new technology and systems designed to enhance ATS;

M. To appropriate agencies, entities, and persons when (1) it is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; (2) DHS has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; and (3) the disclosure is made to such agencies, entities, and persons when reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

The data is stored electronically at the National Data Center for current data and offsite at an alternative data storage facility for historical logs and system backups.

Retrievability:

The data is retrievable by name or personal identifier from an electronic database.

Safeguards:

All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include all of the following: restricting access to those with a "need to know"; using locks, alarm devices, and passwords; compartmentalizing databases; auditing software; and encrypting data communications**.**

ATS also monitors source systems for changes to the source data. The system manager, in addition, has the capability to maintain system back-ups for the purpose of supporting continuity of operations and the discrete need to isolate and copy specific data access transactions for the purpose of conducting security incident investigations. ATS information is secured in full compliance with the requirements of the Federal Information Security Management Act (FISMA) and the DHS IT Security Program Handbook. This handbook establishes a comprehensive information security program.

Use and Control:

CBP maintains full access for a limited number of authorized personnel to all information contained within ATS. Authorized personnel receive thorough background investigations and extensive training on CBP security and privacy policies on the appropriate use of ATS information. These individuals are trained to review the risk assessments and background information to identify individuals who may likely pose a risk. To ensure that ATS is being accessed and used appropriately, audit logs are also created and reviewed routinely by CBP's Office of Internal Affairs to ensure integrity of the system and process.

Access to the risk assessment results and related rules is restricted to a limited number of authorized government personnel who have gone through extensive training on the appropriate use of this information and CBP policies, including for security and privacy. These All individuals are specifically trained to review the risk assessments and background information to identify individuals who may likely pose a risk.

Retention and Disposal:

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 active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases (*i.e.*, specific and

credible threats; flights, individuals, and routes of concern; or other defined sets of circumstances) will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

It is important to note that the justification for a fifteen year retention period 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. 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.

System manager(s) and address:

Executive Director, National Targeting and Security, Office of Field Operations, U.S. Customs and Border Protection, Ronald Reagan Building and Director, Targeting and Analysis, Systems Program Office, Office of Information Technology, U.S. Customs and Border Protection.

Public Record Access/Redress Procedures:

DHS policy allows persons (including foreign nationals) to access and redress under the Privacy Act to raw PNR data maintained in ATS-P. The PNR data, 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, such as . This access does not extend to other information in ATS obtained from official sources (which are covered under separate SORNs) or that is created by CBP, such as the targeting rules and screening results, which are law enforcement sensitive information and are exempt from certain provisions of the Privacy Act. For other information in this system of records, individuals generally may not seek access for purposes of determining if the system contains records pertaining to a particular individual or person. (See 5 U.S.C. 552a (e)(4)(G) and (f)(1)).

Individuals, regardless of nationality, may seek access to records about themselves in accordance with the Freedom of Information Act. In addition, DHS policy allows persons, including foreign nationals, to seek access under the Privacy Act to raw PNR data submitted to ATS-P. Requests for access to personally identifiable information contained in PNR that was provided by the requestor or by someone else on behalf of the requestor, regarding the requestor, may be submitted to the FOIA/PA Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.50C, 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 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-P and other data stored in other DHS databases through one application. Additionally, for further information on ATS and the redress options please see the accompanying PIA for ATS published on the DHS website at www.dhs.gov/privacy. 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 and at www.dhs.gov.

Additionally, a traveler may seek redress from CBP at the time of the border crossing.

Contesting record procedures:

Individuals may seek redress and/or contest a record through several different means, all of which 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.

Record source categories:

The system contains information derived from other law enforcement systems operated by DHS and federal, state, local, tribal, or foreign government agencies, which collected the underlying data from individuals and public entities directly.

The system also contains information collected from carriers that operate vessels, vehicles, aircraft, and/or trains that enter or exit the United States. In addition, the cargo modules (ATS-Inbound and Outbound) employ information collected from third party data aggregators.

Exemptions claimed for the system:

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. 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. 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.

Dated:

Hugo Teufel III,

Chief Privacy Officer.