9110-06

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2012-0019]

Privacy Act of 1974; U.S. Customs and Border Protection, DHS/CBP-006 - Automated Targeting System, System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to update and expand an existing Department of Homeland Security system of records notice titled, U.S. Customs and Border Protection, DHS/CBP-006 - Automated Targeting System (ATS) 72 FR 43650, August 6, 2007. The Department of Homeland Security (DHS) and U.S. Customs and Border Protection (CBP) have designed ATS to efficiently perform risk assessments on information pertaining to international travelers and import and export shipments attempting to enter or leave the United States. ATS uses a rule-managed technology that facilitates the targeting of high-risk travelers and cargo.

DHS/CBP is publishing this System of Records Notice (SORN) to update ATS and to update and expand the categories of individuals, categories of records, routine uses, access provisions, and sources of data stored in ATS. Elsewhere in the Federal Register, the Department of Homeland Security is concurrently issuing a Notice of Proposed Rulemaking exempting this system of records from certain provisions of the

Privacy Act. This updated and expanded system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This system will be effective [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2012-0019 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 703-483-2999.
- Mail: Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Laurence E. Castelli (202-325-0280), CBP Privacy Officer, Office of International Trade, U.S. Customs and Border Protection, Mint Annex, 799 Ninth Street, NW, Washington, DC 20229. For privacy issues please contact: Mary Ellen Callahan (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to update and expand an existing Department of Homeland Security SORN titled, U.S. Customs and Border Protection, DHS/CBP-006 - Automated Targeting System (ATS) 72 FR 43650, August 6, 2007.

This SORN is being updated and expanded to inform the public about changes to the Automated Targeting System (ATS) categories of individuals, categories of records, routine uses, access provisions, and sources of data. DHS/CBP is updating and expanding the categories of individuals, categories of records, and sources of records stored in ATS because it has certain data that it must ingest for performance purposes. The Privacy Impact Assessment (PIA), which DHS will publish on its website (http://www.dhs.gov/privacy) concurrently with the publication of this SORN in the Federal Register, provides a full discussion of the functional capabilities of ATS and its modules. DHS and CBP have previously exempted portions of ATS from the notification, access, amendment, and public accounting provisions of the Privacy Act because it is a law enforcement system. DHS and CBP, however, will consider each request for access to records maintained in ATS to determine whether or not information may be released. DHS and CBP further note that despite the exemption taken on this system of records they are providing access and amendment to passenger name records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. § 44909, as implemented by 19 CFR § 122.49d, Importer Security Filing (10+2 documentation)

information, and any records that were ingested by ATS where the source system of records already provides access and/or amendment under the Privacy Act.

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

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

centric view of all data responsive to a query about the person's identity from the selected databases.

In order to do the above, ATS pulls data from many different source systems. In some instances ATS is the official record for the information, while in other instances ATS ingests and maintains the information as a copy or provides a pointer to the information in the underlying system. Below is a summary:

- *Official Record:* ATS maintains the official record for Passenger Name Records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. § 44909, as implemented by 19 CFR § 122.49d; for Importer Security Filing (10+2 documentation) information, which provides advanced information about cargo and related persons and entities for risk assessment and targeting purposes; for results of Cargo Enforcement Exams; for the combination of license plate, Department of Motor Vehicle (DMV) registration data and biographical data associated with a border crossing; for law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source and/or classified information; and information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department.
- *Ingestion of Data:* ATS maintains copies of key elements of certain CBP databases in order to minimize the processing time for searches on the operational systems and to act as a backup for certain operational systems, including, but not limited to: Automated Commercial Environment (ACE), Automated Commercial System (ACS), Automated Export System (AES),

Advance Passenger Information System (APIS), Border Crossing Information (BCI), Consular Electronic Application Center (CEAC), Enforcement Integrated Database (EID)[which includes the Enforcement Case Tracking System (ENFORCE)], Electronic System for Travel Authorization (ESTA), Global Enrollment System (GES), Non-Immigrant Information System (NIIS), historical National Security Entry-Exit Registration System (NSEERS), Seized Asset and Case Tracking System (SEACATS), U.S. Immigration and Customs Enforcement (ICE) Student Exchange and Visitor Information System (SEVIS), Social Security Administration (SSA) Death Master File, TECS, Terrorist Screening Database (TSDB) through the DHS Watchlist Service (WLS), and WebIDENT. If additional data is ingested and that additional data does not require amendment of the categories of individuals or categories of records in this SORN, the PIA for ATS will be updated to reflect that information. The updated PIA can be found at www.dhs.gov/privacy.

- *Pointer System:* ATS accesses and uses additional databases without ingesting the data, including, but not limited to: CBP Border Patrol Enforcement Tracking System (BPETS), Department of State Consular Consolidated Database (CCD), commercial data aggregators, CBP's Enterprise Geospatial Information Services (eGIS), DHS/USVISIT IDENT, National Law Enforcement Telecommunications System (Nlets), DOJ's National Crime Information Center (NCIC), the results of queries in the FBI's Interstate Identification Index (III), and the National Insurance Crime Bureau's

(NICB's) private database of stolen vehicles. If additional data is ingested and that additional data does not require amendment of the categories of individuals or categories of records in this SORN, the PIA for ATS will be updated to reflect that information. The updated PIA can be found at www.dhs.gov/privacy.

DHS/CBP has reorganized the ATS routine uses to provide greater uniformity across DHS systems. Consistent with DHS's information sharing mission, information stored in ATS may be shared with other DHS components, as well as appropriate federal, state, local, tribal, foreign, or international government agencies. This sharing will only take place after DHS determines that the recipient has a need to know the information to carry out functions consistent with the routine uses set forth in this SORN.

DHS has exempted the system from the notification, access, amendment, and certain accounting provisions of the Privacy Act of 1974 because of the law enforcement nature of ATS. Despite the exemptions taken on this system of records, CBP and DHS are not exempting the following records from the access and amendment provisions of the Privacy Act: passenger name records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. § 44909, as implemented by 19 CFR § 122.49d, Importer Security Filing (10+2 documentation) information, and any records that were ingested by ATS where the source system of records already provides access and/or amendment under the Privacy Act. A traveler may obtain access to his or her PNR and request amendment as appropriate, but records concerning the targeting rules, the responses to rules, case events, law enforcement and/or intelligence data, reports, projects developed by CBP that may include public source and/or classified information, information

obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department, or records exempted from access by the system from which ATS ingested or accessed the information, will not be accessible to the individual.

II. Privacy Act

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 individuals' records. 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 for which information is retrieved by the name of an 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 United States citizens and lawful permanent residents. As a matter of policy (*Privacy Policy Guidance Memorandum 2007-1*, most recently updated January 7, 2009), DHS extends administrative Privacy Act protections to all persons, regardless of citizenship, where a system of records maintains information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR Part 5.

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 in order

to make agency record keeping practices transparent, to notify individuals regarding the uses to which their records are put, and to assist individuals with more easily finding such files within the agency. Below is the description of the U.S. Customs and Border Protection DHS/CBP-006 Automated Targeting System system of records.

In accordance with 5 U.S.C. §552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

System of Records

DHS/ CBP-006

System name:

U.S. Customs and Border Protection Automated Targeting System

Security classification:

Unclassified, sensitive, classified.

System location:

Records are maintained at the CBP Headquarters in Washington, D.C., and can be accessed from field offices and from locations abroad where ATS users are stationed.

Categories of individuals covered by the system:

ATS handles information relating to the following individuals:

A. Persons, including operators, crew, and passengers, who seek to, or do in fact, enter, exit, or transit through the United States or through other locations where CBP maintains an enforcement or operational presence by land, air, or sea.
B. Crew members traveling on commercial aircraft that fly over the United States.

C. Persons who engage in any form of trade or other commercial transaction related to the importation or exportation of merchandise, including those required to submit an Importer Security Filing.

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

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, or on behalf of persons seeking to import, export or ship merchandise through the United States.

F. Owners of vehicles that cross the border.

G. Persons whose data was received by the Department as the result of memoranda of understanding or other information sharing agreement or arrangement because the information is relevant to the border security mission of the Department.

H. Persons who were identified in a narrative report, prepared by an officer or agent, as being related to or associated with other persons who are alleged to be involved in, who are suspected of, or who have been arrested for violations of the laws enforced or administered by DHS.

I. Persons who may pose a threat to the United States.

Categories of records in the system:

ATS contains various types of data to support its targeting missions, incorporating information germane to the identification of individuals, including, but not limited to:

- Name

- Addresses (home, work, and/or destination, as appropriate)
- Telephone and fax numbers
- Tax ID number (*e.g.*, Employer Identification Number (EIN) or Social Security Number (SSN), where available)
- Date and place of birth
- Gender
- Nationality
- Country of Residence
- Citizenship
- Alias
- Physical characteristics, including biometrics where available (*e.g.*, height, weight, race, eye and hair color, scars, tattoos, marks, fingerprints)
- Familial relationships and other contact information
- Property information
- Occupation and employment information
- Biographical and biometric information from or associated with online immigrant and non-immigrant visa applications, including (as available):
    - U.S. sponsor's name, address, and phone number
    - U.S. contact name, address, and phone number
    - Employer name, address, and phone number
    - E-mail address, IP Address, applicant ID
    - Marital Status
    - Alien number

- Social Security Number
- Tax Identification Number
- Organization Name
- U.S. Status
- Income information for Joint Sponsors
- Education, military experience, relationship information
- Responses to vetting questions pertaining to admissibility or eligibility

- Information from documents used to verify the identity of individuals (*e.g.*, driver's license, passport, visa, alien registration, citizenship card, border crossing card, birth certificate, certificate of naturalization, re-entry permit, military card) including the:
  - type
  - number
  - date of issuance
  - place of issuance

The system contains travel information pertaining to individuals, including:

- The combination of license plate, Department of Motor Vehicle (DMV) registration data and biographical data associated with a border crossing
- Information derived from an ESTA application including responses to vetting questions pertaining to admissibility (where applicable)
- Travel itinerary
- Date of arrival or departure, and means of conveyance with associated

identification (*e.g.*, Vehicle Identification Number, year, make, model, registration)

- Passenger Name Record (PNR):
    1. PNR record locator code
    2. Date of reservation/ issue of ticket
    3. Date(s) of intended travel
    4. Name(s)
    5. Available frequent flier and benefit information (*i.e.*, free tickets, upgrades)
    6. Other names on PNR, including number of travelers on PNR
    7. All available contact information (including originator of reservation)
    8. All available payment/billing information (*e.g.*, credit card number)
    9. Travel itinerary for specific PNR
    10. Travel agency/travel agent
    11. Code share information (*e.g.,* when one air carrier sells seats on another air carrier's flight)
    12. Split/divided information (*e.g.*, when one PNR contains a reference to another PNR)
    13. Travel status of passenger (including confirmations and check-in status)
    14. Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote (ATFQ) fields
    15. Baggage information
    16. Seat information, including seat number

17. General remarks including Other Service Indicated (OSI), Special Service Indicated (SSI) and Supplemental Service Request (SSR) information
18. Any collected APIS information (*e.g.,* Advance Passenger Information (API)) that is initially captured by an air carrier within its PNR, such as passport number, date of birth and gender)
19. All historical changes to the PNR listed in numbers 1 to 18

Note: 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 where the life of an individual could be imperiled or seriously impaired.

The system contains information collected for the importation or exportation of cargo and/or property, including:

- Bill of lading
- Commodity type
- License number and license country for Office of Defense Trade Controls registrants
- Inspection and examination results

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

- Manufacturer (or supplier)
- Seller (*i.e.*, full name and address or widely accepted business number such as a Data Universal Numbering System (DUNS) number)
- Buyer (*i.e.*, full name and address)
- Ship to party (full name and/or business name and address)
- Container stuffing location
- Consolidator (stuffer)
- Importer of record number/Foreign Trade Zone applicant identification number
- Consignee number(s)
- Country of origin
- Commodity: Harmonized Tariff Schedule of the United States (HTSUS) number

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

- Booking party (*i.e.*, name and address)
- Foreign port of unlading
- Place of delivery
- Ship to party
- Commodity HTSUS number

The system contains assessments and other information obtained in accordance with the terms of memoranda of understanding or other arrangement because the information is relevant to the border security mission of the Department.

The system also contains information created by CBP, including:

- Admissibility determinations
- Results of Cargo Enforcement Exams
- Law enforcement or intelligence information regarding an individual
- 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
- Assessments resulting from the rules, with a record of which rules were used to develop the assessment
- Operational and analytical reports and/or projects developed that may include public source information and/or classified information obtained by users/analysts for reference or incorporation into the report or project.

Authority for maintenance of the system:

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

Purpose(s):

PURPOSES FOR PNR IN ATS: PNR may be used,

(1.) To prevent, detect, investigate, and prosecute:

a. Terrorist offenses and related crimes, including

i. Conduct that—

1. involves a violent act or an act dangerous to human life, property, or infrastructure; and

2. appears to be intended to –

a. intimidate or coerce a civilian population;

b. influence the policy of a government by intimidation or coercion; or

c. affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking.

ii. Activities constituting an offense within the scope of and as defined in applicable international conventions and protocols relating to terrorism;

iii. Providing or collecting funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the acts described in subparagraphs (i) or (ii);

iv. Attempting to commit any of the acts described in subparagraphs (i), (ii), or (iii);

v. Participating as an accomplice in the commission of any of the acts described in subparagraphs (i), (ii), or (iii);

vi. Organizing or directing others to commit any of the acts described in subparagraphs (i), (ii), or (iii);

vii. Contributing in any other way to the commission of any of the acts described in subparagraphs (i), (ii), or (iii);

viii. Threatening to commit an act described in subparagraph (i) under circumstances which indicate that the threat is credible;

b. Other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature;

A crime is considered as transnational in nature in particular if:

i. It is committed in more than one country;

ii. It is committed in one country but a substantial part of its preparation, planning, direction or control takes place in another country;

iii. It is committed in one country but involves an organized criminal group that engages in criminal activities in more than one country;

iv. It is committed in one country but has substantial effects in another country; or

v. It is committed in one country and the offender is in or intends to travel to another country;

(2) on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court;

(3) to identify persons who would be subject to closer questioning or examination upon arrival to or departure from the United States or who

may require further examination.

(4) for domestic law enforcement, judicial powers, or proceedings, where violations of law or indications thereof are detected in the course of the use and processing of PNR.

PURPOSES OF ATS (EXCEPT for PNR):

ATS uses all other data for purposes listed above as well as below:

(a) To perform targeting of individuals who may pose a risk to border security or public safety, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law;

(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 system, including categories of users and the purposes of such uses:

Information ingested into this system from another source system is to be handled consistent with the published system of records notice for the source system and will continue to be governed by the routine uses for that source system. The routine uses below apply only to records that are maintained as official records in ATS (*i.e.*, records which are maintained in ATS that are not covered by other originating systems of record, including: PNR; Importer

Security Filings; Cargo Enforcement Exams; the combination of license plate, Department of Motor Vehicle (DMV) registration data and biographical data associated with a border crossing; law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information and/or classified information; and information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department). With respect to PNR, DHS only discloses information to those authorities who intend to use the information consistent with the purposes identified above, and have sufficient capability to protect and safeguard the information. 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) as follows:

A. To the Department of Justice (including United States Attorney Offices) or other federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary or relevant to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. any employee of DHS in his/her official capacity;

3. any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or

4. the United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made pursuant to a written Privacy Act waiver at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

D. To an agency or organization for the purpose 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.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has 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, of identity theft or fraud, or of harm to the security or integrity of this system or of harm to other systems or programs (whether maintained by DHS or another agency or entity) or harm to the individuals that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is 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.

F. To contractors and their agents, 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. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To appropriate federal, state, tribal, local, 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;

H. To federal and foreign government intelligence or counterterrorism agencies or components where DHS becomes aware of an indication of a threat or potential threat to national or international security, or to assist in anti-terrorism efforts;

I. To an organization or person 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 person;

J. 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;

K. 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;

L. 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;

M. 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;

N. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Disclosure to consumer reporting agencies:

None.

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

Storage:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on magnetic disc, tape, digital media, and CD-ROM.

Retrievability:

Records may be retrieved by any of the data elements described in "Categories of Records," including by name or personal identifier from an electronic database.

Safeguards:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

Retention and disposal:

Official Records in this system (Passenger Name Records (PNR); Importer Security Filings (10+2 documentation); results of Cargo Enforcement Exams; the combination of license plate, Department of Motor Vehicle registration data, and biographical data associated with a border crossing; law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information and/or classified information; and information obtained through memoranda

of understanding or other arrangements because the information is relevant to the border security mission of the Department will be retained and disposed of in accordance with a records schedule approved by the National Archives and Records Administration on April 12, 2008. ATS collects information directly, ingests information from various systems, and accesses other systems without ingesting the data. To the extent information is ingested from other systems, data is retained in ATS in accordance with the record retention requirements of those systems, or the retention period for ATS, whichever is shortest.

The retention period for the official records maintained in ATS will not exceed fifteen years, after which time the records will be deleted, except as noted below. The retention period for PNR will be subject to the following further access restrictions: ATS users with PNR access will have access to PNR in an active database for up to five years, during which time the PNR will be depersonalized following the first six months retention. After this initial five-year retention, the PNR data will be transferred to a dormant database for a period of up to ten years. PNR data in dormant status will be subject to additional controls including the requirement of obtaining access approval from a senior DHS official designated by the Secretary of Homeland Security. Furthermore, PNR in the dormant database may only be repersonalized in connection with a law enforcement operation and only in response to an identifiable case, threat, or risk. Such limited access and use for older PNR strikes a reasonable balance between protecting this information and allowing CBP to continue to identify potential high-risk travelers. Notwithstanding the foregoing, information maintained only in ATS that is linked to 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.

The justification for a fifteen-year retention period for the official records is based on CBP's law enforcement and security functions at the border. This retention period is based on CBP's historical encounters with suspected terrorists and other criminals, as well as the broader expertise of the law enforcement and intelligence communities. It is well known, for example, that potential terrorists may make multiple visits to the United States in advance of performing an attack. It is over the course of time and multiple visits that a potential risk becomes clear. Travel records, including historical records, are essential in assisting CBP Officers with their risk-based assessment 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 and address:

Executive Director, Automation and Targeting Division, Office of Intelligence and Investigative Liaison, U.S. Customs and Border Protection, and Director, Targeting and Analysis, Systems Program Office, Office of Information and Technology, U.S. Customs and Border Protection, both of whom are located at 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229.

Notification procedure:

The Secretary of Homeland Security has exempted this system from the notification, access, amendment, and certain accounting procedures of the Privacy Act because it is a law enforcement system. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records with appropriate exemptions in place. To the extent that a record is exempted in a source system, the exemption will continue to apply. Despite the exemptions taken on this system of records, CBP and DHS are not exempting the following records from the access and amendment provisions of the Privacy Act: passenger name records (PNR) collected by CBP pursuant to its statutory authority, 49 U.S.C. § 44909, as implemented by 19 CFR § 122.49d; Importer Security Filing (10+2 documentation) information; and any records that were ingested by ATS where the source system of records already provides access and/or amendment under the Privacy Act. Individuals seeking notification of and access to records contained in this system of records, or seeking to contest its content, may submit a request in writing to the Headquarters or CBP FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0655, Washington, D.C. 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must

sign your request, and your signature must either be notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, http://www.dhs.gov or 1-866-431-0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you,
- Identify which component(s) of the Department you believe may have the information about you,
- Specify when you believe the records would have been created,
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records, and
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

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

Record access procedures:

See "Notification procedure" above.

Contesting record procedures:

See "Notification procedure" above.

Record source categories:

Records are ingested from other DHS and federal systems, and from foreign governments (in accordance with the terms of international agreements and arrangements), including but not limited to ACE, ACS, AES, APIS, BCI, CEAC (including Forms DS-160 and DS-260), ENFORCE, ESTA, GES, NIIS, NSEERS, SEACATS, SEVIS, TECS, TSDB-WLS, Social Security Administration's Death Master File, and WebIDENT, Additionally, PNR is obtained from travel reservation systems of commercial carriers. Information from Importer Security Filings is received from importers and ocean carriers. Records are accessed from BPETS, CCD, eGIS, NCIC, and Nlets. Also, the results of queries in the FBI's Interstate Identification Index (III), the National Insurance Crime Bureau's (NICB's) private database of stolen vehicles, and commercial data aggregators are stored in ATS. Lastly, records are also developed from analysis created by users as a result of their use of the system.

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). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, pursuant to 5 U.S.C. § 552a (k)(1) and (k)(2): 5 U.S.C. § 552a(c)(3); (d)(1), (d)(2), (d)(3), and (d)(4); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f).

Despite the exemptions taken on this system of records, CBP and DHS are not exempting the following records from the access and amendment provisions of the Privacy Act: passenger name records (PNR) collected by CBP pursuant to its statutory

authority, 49 U.S.C. § 44909, as implemented by 19 CFR § 122.49d; Importer Security Filing (10+2 documentation) information; and any records that were ingested by ATS where the source system of records already provides access and/or amendment under the Privacy Act. A traveler may obtain access to his or her PNR, but records concerning the targeting rules, the responses to rules, case events, law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information and/or classified information, information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department, or records exempted from access by the system from which ATS ingested or accessed the information will not be accessible to the individual.

Mary Ellen Callahan

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2012-12396 Filed 05/21/2012 at 8:45 am; Publication Date: 05/22/2012]