[Federal Register: November 2, 2006 (Volume 71, Number 212)]
[Notices]
[Page 64543-64546]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr02no06-51]

==========

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[DHS-2006-0060]

Privacy Act of 1974; System of Records

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of Privacy Act system of records.

SUMMARY: To provide expanded notice and transparency to the public, the Department of Homeland Security, U.S. Customs and Border Protection gives notice regarding the Automated Targeting System, which is the enforcement screening module associated with the Treasury Enforcement Communications System and was previously covered by the Treasury Enforcement Communications System ``System of Records Notice.'' This system of records is subject to the Privacy Act of 1974, as amended (5 U.S.C. 552a).

The Treasury Enforcement Communications System is established as an overarching law enforcement information collection, targeting, and sharing environment. This environment is comprised of several modules designed to collect, maintain, and screen data, conduct targeting, and share information. Among these modules, the Automated Targeting System performs screening of both inbound and outbound cargo, travelers, and conveyances. As part of this screening function, the Automated Targeting System compares information obtained from the public with a set series of queries designed to permit targeting of conveyances, goods, cargo, or persons to facilitate DHS's border enforcement mission.

The risk assessment and links to information upon which the assessment is based, which are stored in the Automated Targeting System, are created from existing information in a number of sources, including, but not limited to: the trade community through the Automated Commercial System or its successor; the Automated Commercial Environment system; the traveling public through information submitted by their carrier to the Advance Passenger Information System; persons crossing the United States land border by automobile or on foot; the Treasury Enforcement Communications System, or its successor; or law enforcement information maintained in other parts of the Treasury Enforcement Communications System that pertain to persons, goods, or conveyances.

As part of the information it accesses for screening, Passenger Name Record (PNR) information, which is currently collected pursuant to an existing CBP regulation (19 CFR 122.49d) from both inbound and outbound travelers through the carrier upon which travel occurs, is stored in the Automated Targeting System. PNR is comprised of data

which carriers collect as a matter of their usual business practice in negotiating and arranging the travel transaction.

As noted above, this system of records notice does not identify or create any new collection of information, rather DHS is providing additional notice and transparency of the functionality of these systems.

DATES: The new system of records will be effective December 4, 2006, unless comments are received that result in a contrary determination.

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

Federal eRulemaking Portal: http://www.regulations.gov.

Follow the instructions for submitting comments via docket number DH6-2006-0060.

Fax: 202-572-8727.

Mail: Comments by mail are to be addressed to the Border Security Regulations Branch, Office of Regulations and Rulings, Bureau of Customs and Border Protection, 1300 Pennsylvania Avenue, NW. (Mint Annex), Washington, DC 20229. Comments by mail may also be submitted to Hugo Teufel III, Chief Privacy Officer, Department of Homeland Security, 601 S. 12th Street, Arlington, VA 22202-4220.

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.

Submitted comments may also be inspected during regular business days between the hours of 9 a.m. and 4:30 p.m. at the Regulations Branch, Office of Regulations and Rulings, Bureau of Customs and Border Protection, 799 9th Street, NW., 5th Floor, Washington, DC. Arrangements to inspect submitted comments should be made in advance by calling Mr. Joseph Clark at (202) 572-8768.

[[Page 64544]]

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Laurence E. Castelli (202-572-8790), Chief, Privacy Act Policy and Procedures Branch, Bureau of Customs and Border Protection, Office of Regulations & Rulings, Mint Annex, 1300 Pennsylvania Ave., NW., Washington, DC 20229. For privacy issues please contact: Hugo Teufel III (571-227-3813), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION: Bureau of Customs and Border Protection (CBP), Department of Homeland Security (DHS), has traditionally relied on computerized cargo screening processes to aid the CBP inspection workforce in the cargo release process. Separately, CBP has used the advance submission of traveler information to aid in screening travelers to facilitate its border enforcement mission. The Automated Targeting System (ATS) associates information obtained from CBP's cargo, travelers, and border enforcement systems with a level of risk posed by each item and person as determined through the rule based query of the cargo or personal information accessed by ATS.

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 United States citizens and legal permanent residents. ATS involves the collection and creation of information that is maintained in a system of records.

Previously, this information was covered by the Treasury Enforcement Communications System (TECS) system of records notice, as ATS is a functional module associated with the environment of TECS. ATS is employed as an analytical tool to enhance CBP screening and targeting capabilities by permitting query-based comparisons of different data modules associated with the TECS system, as well as comparisons with data sets from sources outside of TECS. 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, CBP has determined that ATS should be noticed as a separate system of records, giving greater visibility into its targeting and screening efforts.

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 recordkeeping practices transparent, to notify individuals regarding the uses to which personally identifiable information is put, and to assist the individual to more easily find such files within the agency.

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.

DHS/CBP-006

SYSTEM NAME:

Automated Targeting System (ATS)--DHS/CBP.

SYSTEM LOCATION:

This computer database is located at the Bureau of Customs and Border Protection (CBP) National Data Center in Washington, DC. Computer terminals are located at customhouses, border ports of entry, airport inspection facilities under the jurisdiction of the Department of Homeland Security (DHS) and other locations at which DHS authorized personnel may be posted to facilitate DHS's mission.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

A. Persons seeking to enter or exit 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; and

D. Persons who serve as operators, crew, or passengers on any vessel, vehicle, aircraft, or train who enters or exits the United States.

CATEGORIES OF RECORDS IN THE SYSTEM:

ATS builds a risk assessment for cargo, conveyances, and travelers based on criteria and rules developed by CBP. ATS maintains the resulting assessment 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. This assessment and related rules history associated with developing a risk assessment for an individual are maintained for up to forty years to support ongoing targeting requirements.

ATS--P (Automated Targeting System--Passenger), a component of ATS, maintains the PNR information obtained from commercial carriers for purposes of assessing the risk of international travelers. PNR may include such items as:

- PNR record locator code,
- Date of reservation,
- Date(s) of intended travel,
- Name,
- Other names on PNR,
- Number of travelers on PNR,
- Seat information,
- Address,
- All forms of payment information,
- Billing address,
- Contact telephone numbers,
- All travel itinerary for specific PNR,
- Frequent flyer information,
- Travel agency,
- Travel agent,
- Code share PNR information,
- Travel status of passenger,
- Split/Divided PNR information,
- Identifiers for free tickets,
- One-way tickets,
- E-mail address,
- Ticketing field information,
- Automated Ticketing Fare Quote (ATFQ) fields,
- General remarks,
- Ticket number,
- Seat number,
- Date of ticket issuance,
- Any collected APIS information,
- No show history,
- Number of bags,
- Bag tag numbers,
- Go show information,
- Number of bags on each segment,
- Other Supplementary information (OSI),
- Special Services information (SSI),
- Special Services Request (SSR),
- Voluntary/involuntary upgrades,
- Received from information, and
- All historical changes to the PNR

Not all carriers maintain the same sets of information for PNR.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

19 U.S.C. 482, 1461, 1496, and 1581-1582, 8 U.S.C. 1357, Title VII of Public Law 104-208, and 49 U.S.C. 44909.

Purpose(s):

(a) To perform targeting of individuals, including passengers and

[[Page 64545]]

crew, focusing CBP resources by identifying persons who may pose a risk to border security, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law;

(b) To perform targeting 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 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:

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 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 civil or criminal laws;

B. To appropriate Federal, state, local, tribal, or foreign governmental agencies maintaining civil, criminal, or other relevant enforcement information or other pertinent information, which has requested information relevant or necessary to the requesting agency's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure;

C. 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;

D. 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 to the proper performance of the official duties of the officer making the disclosure;

E. To an agency, organization, or individual for the purposes of performing audit or oversight operations as authorized by law;

F. 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;

G. To contractors, grantees, experts, consultants, students, 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;

H. 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, to the extent the information is relevant to the protection of life or property and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure;

I. To the United States 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 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;

J. 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. 2904 and 2906;

K. To appropriate Federal, state, local, tribal, or foreign governmental agencies, if necessary to obtain information relevant to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit and disclosure is appropriate to the proper performance of the official duties of the individual making the disclosure;

L. To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations, for purposes of assisting such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or for combatting other significant public health threats;

M. 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;

N. 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 border security or identify other violations of law;

O. 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) CBP 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 CBP 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 the CBP'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,

[[Page 64546]]

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 DHS IT Security Program Handbook. This handbook establishes a comprehensive information security program.

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 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 created and reviewed routinely by CBP's Office of Internal Affairs.

RETENTION AND DISPOSAL:

The information initially collected in ATS is used for entry screening 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 specifically maintained in ATS will not exceed forty years at which time it will be deleted from ATS. Up to forty years of data retention may be required to cover the potentially active lifespan of individuals associated with terrorism or other criminal activities. The touchstone for data retention, however, is its 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 profile changes in the future, for example, if terrorist associations are identified. Additionally, certain data collected directly by ATS may be subject to shorter retention limitations pursuant to separate arrangements. The adoption of shorter retention periods may not be publicly disclosed if DHS concludes that disclosure would affect operational security, for example by giving terrorism suspects the certainty that their past travel patterns would no longer be known to U.S. authorities.

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.

NOTIFICATION PROCEDURE:

Generally, this system of records may not be accessed for purposes

of determining if the system is a record pertaining to a particular individual. (See 5 U.S.C. 552a(e)(4)(G) and (f)(1)).

General inquiries regarding ATS may be directed to the Customer Satisfaction 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).

RECORD ACCESS PROCEDURES:

Generally, this system of records may not be accessed under the Privacy Act for the purpose of inspection. The majority of this system is exempted from this requirement pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

General inquiries regarding ATS may be directed to the Customer Satisfaction Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5-C, 1300 Pennsylvania Avenue, NW., Washington, DC 20229.

Requests should conform to the requirements of 6 CFR Part 5, Subpart B, 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.

CONTESTING RECORD PROCEDURES:

Since this system of records may not be accessed, generally, for purposes of determining if the system contains a record pertaining to a particular individual and those records, if any, cannot be inspected, the system may not be accessed under the Privacy Act for the purpose of contesting the content of the record.

RECORD SOURCE CATEGORIES:

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

In addition, the system contains information collected from carriers that operate vessels, vehicles, aircraft, and/or trains that enter or exit the United States.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Pursuant to 31 CFR 1.36 pertaining to the Treasury Enforcement Communications System, the Automated Targeting System, which was previously covered by the Treasury Enforcement Communications System (TECS) system of records notice and associated with the below exemptions, records and information in this system are exempt from 5 U.S.C. 552a(c)(3), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(4)(G), (H), and (I), and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). DHS intends to review these exemptions and, if warranted, issue a new set of exemptions specific to ATS within ninety (90) days of the publication of this notice.

Dated: October 27, 2006.

Hugo Teufel III,

Chief Privacy Officer.

[FR Doc. 06-9026 Filed 10-30-06; 3:31 pm]

BILLING CODE 4410-10-P