DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[DHS–2007–0041]

Privacy Act of 1974; Customs and Border Protection Advanced Passenger Information System Systems of Records

AGENCY: Privacy Office; DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: Pursuant to the Privacy Act of 1974, the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) gives notice that it is establishing a new system of records for collecting certain biographical information on all passenger and crew members who arrive in or depart from, or transit through (and crew that over fly) the United States on a covered air or vessel carrier, and, in the case of crew members, those who continue domestically on a foreign air or vessel carrier. The system of records is the Advance Passenger Information System.

Previously, this information was maintained within the Treasury Enforcement Communications System and was covered by a system of records notice published for the Treasury Enforcement Communications System. CBP is publishing a new system of records notice in order to permit the traveling public greater access to individual information and a more complete understanding of how and where information pertaining to them is collected and maintained.

DATES: The new system of records will be effective September 24, 2007.

ADDRESSES: You may submit comments, identified by Docket Number DHS–2007–0041 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* 1–866–466–5370.
- *Mail:* Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 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 (202–572–8790), Chief, Privacy Act Policy and Procedures Branch, U.S. Customs and Border Protection, Office of International Trade, Regulations & Rulings, Mint Annex, 1300 Pennsylvania Ave., NW., Washington, DC 20229. For privacy issues contact: Hugo Teufel III (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

The Advance Passenger Information System (APIS) was originally developed as a voluntary program by the former U.S. Customs Service (Customs Service) in 1988 in cooperation with the former U.S. Immigration and Naturalization Service (INS) and the airline industry. Previously, this information was maintained within the Treasury Enforcement Communications System (TECS) and was covered by a system of records notice published for TECS. The most recent TECS SORN was published at 66 FR 52984 (Oct 18, 2001). In the original APIS regulation, commercial air and vessel carriers collected passengers' biographical data and transmitted the data to the Customs Service while the flight or the vessel was en route to the United States. The Customs Service Data Center used APIS data to perform a check against CBP's law enforcement databases, as well as information from the Federal Bureau of Investigations Terrorist Screening Center's Terrorist Screening Database (TSDB), information on individuals with outstanding wants or warrants, and information from other government agencies regarding high risk parties. Through the legacy voluntary APIS data program, checks were performed in advance of the arrival of the aircraft or vessel. The results were referenced by Customs agents or inspectors once the passengers arrived. This resulted in a significant time savings for the clearance of passengers and carriers.

The Aviation and Transportation Security Act of 2001 and the Enhanced Border Security and Visa Entry Reform Act of 2002 provided specific authority for the mandatory collection of certain information on all passenger and crewmembers that arrive in or depart from the United States on a commercial air or vessel carrier. The information is required to be collected and submitted to CBP as APIS data.

The information that is required to be collected and submitted to the APIS can be found on routine arrival/departure documents that passengers and crewmembers must provide to CBP, when entering or departing the United States. APIS includes complete name, date of birth, gender, country of citizenship, passport/alien registration number and country of issuance, passport expiration date, country of residence, status on board the aircraft, travel document type, United States destination address (except for U.S. Citizens, lawful permanent residents, crew and those in transit), place of birth and address of permanent residence (flight crew only), pilot certificate number and country of issuance (flight crew only, if applicable) and the Passenger Name Record (PNR) locator number. The PNR locator number allows CBP to access PNR consistent with its regulatory authority under 19 CFR 122.49d.

Additionally, air and vessel carriers must provide the airline carrier code, flight number, vessel name, vessel country of registry/flag, International Maritime Organization number or other official number of the vessel, voyage number, date of arrival/departure, foreign airport/port where the passengers and crew members began their air/sea transportation to the United States; for passengers and crew members destined for the United States, the location where the passengers and crew members will undergo customs and immigration clearance by CBP; and for passengers and crew members that are transiting through (and crew on flights over flying) the United States and not clearing CBP, the foreign airport/port of ultimate destination, and status on board (whether an individual is crew or non-crew); and for passengers and crew departing the United States, the final foreign airport/port of arrival.

CBP will collect the passengers' and crewmembers' information that is supplied by the air or vessel carriers in advance of a passenger's and crewmember's arrival in or departure from (and, for crew on flights over flying) the United States and maintains this information in the Advance Passenger Information System. The information will be used to perform counterterrorism, law enforcement, and public security queries to identify risks to the aircraft or vessel, to its occupants, or to the United States and to expedite CBP processing.

Under the Final Rule revision to APIS (70 FR 17820 (Apr. 7, 2005)), CBP mandates that air and vessel carriers collect personally identifiable information about passengers and crewmembers (including ''non-crew'' as defined in the 2005 APIS Final Rule) traveling by air or sea, and arriving in,

or departing from (and, in the case of crew, flights overflying), the United States from the respective carriers—this information is often collected and maintained on what is referred to as the manifest. The information that is required to be collected and submitted to APIS can be found on routine travel documents that passengers and crewmembers must provide when processed into or out of the United States (and most of the information is included on the Machine Readable Zone (MRZ) of most passports).

The purpose of the information collection is to screen passengers and crew members arriving from foreign travel points and departing the United States to identify those persons who may pose a risk to border, aviation or public security, may be a terrorist or suspected terrorist or affiliated with or suspected of being affiliated with terrorists, may be inadmissible, may be a person of interest, or may otherwise be engaged in activity in violation of U.S. law, or the subject of wants or warrants. The system allows CBP to facilitate effectively and efficiently the entry and departure of legitimate travelers into and from the United States. Using APIS, DHS officers can quickly reference the results of the advanced research that has been conducted through CBP's law enforcement databases, including information from the TSDB and information on individuals with outstanding wants or warrants, confirm the accuracy of that information by comparison with information obtained from the traveler (passenger and crew) and from the carriers, and make immediate determinations as to a traveler's security risk, admissibility and other determinations bearing on CBP's inspectional and screening processes.

Information collected in APIS is maintained for a period of no more than twelve months from the date of collection at which time the data is erased from APIS. Following CBP processing, a copy of certain information is transferred to the Border Crossing Information System, a subsystem of TECS. During physical processing at the border, primary inspection lane and ID inspector are added to APIS and the APIS information is verified. This information derived from APIS includes: complete name, date of birth, gender, date of arrival, date of departure, time arrived, means of arrival (air/sea), travel document, departure location, airline code, flight number, and the result of the CBP processing. Additionally, for individuals subject to US-VISIT requirements, a copy of certain APIS data is transferred to the Arrival and Departure Information System (ADIS) for effective and efficient tracking of foreign nationals, including to help identify lawfully admitted non-immigrants who remain in the United States beyond the period of authorized stay. US-VISIT currently applies to all visitors (with limited exemptions). The SORN for ADIS was last published on December 12, 2003 (68 FR 69412). The information transferred from APIS to ADIS includes: Complete name, date of birth, gender, citizenship, country of residence, status on board the vessel, U.S. destination address, passport number, expiration date of passport, country of issuance (for non-immigrants authorized to work), alien registration number, port of entry, entry date, port of departure, and departure date.

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 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 lawful permanent residents. APIS involves the collection of information that will be maintained in a system of records.

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, and to assist the individual to more easily find such files within the agency. Below is the description of system of records referred to as the Advanced Passenger Information 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–005

SYSTEM NAME:

Advanced Passenger Information System (APIS)

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

This computer database is located at U.S. 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. Terminals may also be located at appropriate facilities for other participating government agencies.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this notice consist of:

A. Passengers who arrive and depart the United States by air or sea, including those in transit through the United States or beginning or concluding a portion of their international travel by flying domestically within the United States,

B. Crew members who arrive and depart the United States by air or sea, including those in transit through the United States or beginning or concluding a portion of their international travel by flying domestically within the United States, and

C. Crew members on aircraft that overfly the United States.

CATEGORIES OF RECORDS IN THE SYSTEM:

The records in the database are comprised of the following information: complete name, date of birth, gender, country of citizenship, passport/alien registration number and country of issuance, passport expiration date, country of residence, status on board the aircraft, travel document type, United States destination address (except for U.S. Citizens, lawful permanent residents, crew and those in transit), place of birth and address of permanent residence (flight crew only), pilot certificate number and country of issuance (flight crew only, if applicable), the PNR locator number, primary inspection lane, ID inspector, and records containing the results of comparisons of individuals to information maintained in CBP's law enforcement databases, as well as information from the TSDB, information on individuals with outstanding wants or warrants, and information from other government agencies regarding high risk parties.

In addition, carriers or operators covered by the APIS rules must transmit

to CBP the following information: airline carrier code, flight number, vessel name, vessel country of registry/flag, International Maritime Organization number or other official number of the vessel, voyage number, date of arrival/departure, foreign airport/port where the passengers and crew members began their air/sea transportation to the United States; for passengers and crew members destined for the United States, the location where the passengers and crew members will undergo customs and immigration clearance by CBP; and for passengers and crew members that are transiting through (and crew on flights over flying) the United States and not clearing CBP, the foreign airport/port of ultimate destination; and for passengers and crew departing the United States, the final foreign airport/port of arrival.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The Aviation and Transportation Security Act of 2001, the Enhanced Border Security and Visa Reform Act of 2002, and the Intelligence Reform and Terrorism Prevention Act of 2004, also the Tariff Act of 1930, as amended, including 19 U.S.C. 58b, 66, 1431, 1433, 1436, 1448, 1459, 1590, 1594, 1623, 1624, 1644, and 1644a.

PURPOSE(S):

The purpose of the collection is to screen passengers and crew arriving in, transiting through and departing from (and in the case of crew, overflying) the United States to identify those passengers and crew who may pose a risk to border, aviation or public security, may be a terrorist or suspected terrorist or affiliated with or suspected of being affiliated with terrorists, may be inadmissible, may be a person of interest, or may otherwise be engaged in activity in violation of U.S. law, or the subject of wants or warrants.

APIS allows CBP to facilitate more effectively and efficiently the entry of legitimate travelers into the United States and the departure of legitimate travelers from the United States. As travelers prepare to depart for or from the United States, DHS officers, using APIS, can quickly cross-reference the results of the advanced research that has been conducted through CBP's law enforcement databases, as well as using information from the TSDB, information on individuals with outstanding wants or warrants, and information from other government agencies regarding high risk parties, confirm the accuracy of that information by comparison of it with information obtained from the traveler and from the carriers, and make immediate determinations with regard to the traveler's security risk, admissibility and other determinations bearing on CBP's inspectional and screening processes.

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 DHS believes the information would assist enforcement of 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, to the extent the information is relevant to the protection of life, property or other vital interests of a data subject and 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 for combating 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 an 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 an appropriate Federal, state, local, tribal, territorial, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary 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 when disclosure is appropriate to the proper performance of the official duties of the person making the request;

J. 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;

K. 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: (1) DHS, or (2) any employee of DHS in his/her official capacity, or (3) any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent said employee, or (4) the United States or any agency thereof;

L. 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;

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 border security or identify other violations of law;

N. 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.

O. To the carrier, who submitted traveler, passenger, or crew information to CBP, but only to the extent that CBP provides a message indicating that the individual is ''cleared'' or ''not cleared'' to board the aircraft or depart on the vessel in response to the initial transmission of information, or is identified as a ''selectee''.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

The data is stored electronically at the CBP 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 other unique personal identifier from an electronic database.

SAFEGUARDS:

Information in this system is safeguarded in accordance with applicable laws, rules, and policies. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include role-based access provisions, restricting access to authorized personnel who have a need-to-know, using locks, and password protection identification features. DHS file areas are locked after normal duty hours and the facilities are protected from the outside by security personnel.

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.

All communication links with the CBP datacenter are encrypted. The Databases are fully Certified and Accredited in accordance with the requirements of the Federal Information Security Management Act (FISMA).

Although separate notice is being provided for APIS, it continues to operate within the TECS information technology system architecture; therefore APIS's technical infrastructure is covered by the approved TECS Certification and Accreditation under the National Institute of Standards and Technology. The last certification was in January 2006.

RETENTION AND DISPOSAL:

Information collected in APIS is maintained in this system for a period of no more than twelve months from the date of collection at which time the data is erased from APIS. As part of the vetting and CBP clearance (immigration and customs screening and inspection) of a traveler, information from APIS is copied to the Border Crossing Information System, a subsystem of TECS. Additionally, for individuals subject to US–VISIT requirements, a copy of certain APIS data is transferred to the Arrival and Departure Information System (ADIS) for effective and efficient processing of foreign nationals. The SORN for ADIS was last published on December 12, 2003 (68 FR 69412). Different retention periods apply for APIS data contained in those systems.

SYSTEM MANAGER(S) AND ADDRESS

Director, Office of Automated Systems, U.S. Customs and Border Protection Headquarters, 1300 Pennsylvania Avenue, NW., Washington, DC 20229.

NOTIFICATION PROCEDURES:

DHS allows persons (including foreign nationals) to seek administrative access under the Privacy Act to information maintained in APIS. Persons may only seek access to APIS data that has been provided by the carrier and of which they are the subject. To determine whether APIS contains records relating to you, write to the FOIA/Privacy Act 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).

RECORD ACCESS PROCEDURES:

Requests for notification or access must be in writing and should be addressed to the FOIA/Privacy Act Branch, 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 and can be found at *http://www.dhs.gov/foia.* 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.

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

CONTESTING RECORD PROCEDURES:

Individuals may seek redress and/or contest a record through several different means that 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/Privacy Act 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). 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 *http://www.dhs.gov/trip.*

RECORD SOURCE CATEGORIES:

The system contains data received from aircraft operators/carriers and vessel carriers regarding passengers and crewmembers who arrive in, depart from, transit through or overfly (in the case of flight crew only) the United States on an air or vessel carrier covered by APIS regulations. During physical processing at the border, primary inspection lane and ID inspector are added to APIS, and the APIS information is verified using the travel documents. Additionally, records contain the results of comparisons of individuals to information maintained in CBP law enforcement databases, as well as information from the TSDB, information on individuals with outstanding wants or warrants, and information from other government agencies regarding high risk parties.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

No exemption shall be asserted with respect to information maintained in the system that is collected from a person and submitted by that person's air or vessel carrier, if that person, or his or her agent, seeks access or amendment of such information.

This system, however, may contain records or information recompiled from or created from information contained in other systems of records, which are exempt from certain provisions of the Privacy Act. For these records or information only, in accordance with 5 U.S.C. 552a (j)(2), and (k)(2), DHS will also claim the original exemptions for these records or information from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (5), and (8); (f), and (g) of the Privacy Act of 1974, as amended, as necessary and appropriate to protect such information.

Dated: August 8, 2007.

Hugo Teufel III,

Chief Privacy Officer.

[FR Doc. E7–15976 Filed 8–22–07; 8:45 am]

BILLING CODE 4410–10–P