[Federal Register Volume 80, Number 49 (Friday, March 13, 2015)]
[Notices]
[Pages 13407-13413]
From the Federal Register Online via the Government Publishing Office [www.gpo.gov]
[FR Doc No: 2015-05798]

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2015-0009]

Privacy Act of 1974; Department of Homeland Security/United States Customs and Border Protection Advanced Passenger Information System Systems of Records

AGENCY: Privacy Office, Department of Homeland Security.

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 reissue a current Department of Homeland Security system of records titled, ``Department of Homeland Security/United States Customs and Border Protection-005 Advanced Passenger Information System Systems of Records.'' This system of records allows the Department of Homeland Security/United States Customs and Border Protection to collect and maintain records on certain biographical information on all passengers and crew members who arrive in, depart from, or transit through (and crew that fly over) 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, to additionally encompass private aircraft, rail, and bus travel. This system of records notice has been updated to include changes to security classification, system location, purpose(s), storage, retention and disposal, routine uses, and notification procedure. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. This updated system will be included in the Department of Homeland Security's inventory of record systems, located on the Department of Homeland Security Web site at http://www.dhs.gov/system-records-notices-sorns.

DATES: The system of records will be effective April 13, 2015.

ADDRESSES: You may submit comments identified by docket number DHS-2015-0009 by one of the following methods:
Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
Fax: 202-343-4010.
Mail: Karen L. Neuman, 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: John Connors, (202) 344-1610, Privacy Officer, United States Customs and Border Protection, Privacy and Diversity Office, 1300 Pennsylvania Ave. NW., Washington, DC 20229. For privacy questions, please contact: Karen L. Neuman, (202) 343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the DHS/CBP proposes to update and reissue a current DHS system of records titled, Department of Homeland Security (DHS), United States Customs and Border Protection (CBP)-005 Advanced Passenger Information System (APIS) System of Records. The Aviation and Transportation Security Act of 2001 and the Enhanced Border Security and Visa Entry Reform Act of 2002 provide specific authority for the mandatory collection of certain information about all passenger and crewmembers that arrive in or depart from the United States via private aircraft, commercial air, or vessel carrier. CBP requires that carriers collect and submit information is required to be collected and submitted to CBP as APIS data pursuant to existing regulations. Additionally, rail and bus carriers may provide voluntarily similar, information pertaining to their passengers and crew who arrive in or depart from the United States. References to the types of information that are required to be submitted in the air or vessel environment also pertain to the types of information that may be voluntarily provided in the rail and bus environments.

The information that CBP requires carriers to collect and submit to APIS (as well as information that may be provided voluntarily by bus and rail carriers) can be found on routine arrival/departure documents that passengers and crewmembers must provide to CBP when entering or

departing the United States. APIS

[[Page 13408]]

information 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, vessel, or train; travel document type; U.S. destination address (for all private aircraft passengers and crew, and commercial air, rail, and vessel passengers except for U.S. citizens, lawful permanent residents, crew, and those in transit); place of birth and address of permanent residence (commercial 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 and the system of records notice (SORN) for the Automated Targeting System, DHS/CBP-006 (72 FR 43650, published August 6, 2007).

Additionally, commercial 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 commercial aviation passengers and crew members destined for the United States, the location where the passenger and crew members must undergo customs and immigration clearance by CBP; for commercial passengers and crew members that are transiting through (and crew on aircraft flying over) the United States and not clearing CBP must provide the foreign airport/port of ultimate destination, and status on board (whether an individual is crew or non-crew); and for commercial passengers and crew departing the United States, must provide the final foreign airport/port of arrival. Lastly, pilots of private aircraft must provide the aircraft registration number; type of aircraft; call sign (if available); CBP issued decal number (if available); place of last departure (International Civil Aviation Organization (ICAO) airport code, when available); date and time of aircraft arrival (or departure, for departure notice), estimated time and location of crossing U.S. border/coastline; name of intended airport of first landing; \1\ owner/lessee name (first, last and middle, if available, or business entity name); owner/lessee address (number and street, city, state, zip code, country, telephone number, fax number, and email address); pilot/private aircraft pilot name (last, first and middle, if available); pilot license number; pilot street address (number and street, city state, zip code, country, telephone number, fax number and email address); pilot license country of issuance; operator name (for individuals: last, first and middle, if available, or name of business entity, if available); operator street address (number and street, city, state, zip code, country, telephone number, fax number, and email address); aircraft color(s); complete itinerary (foreign airport landings within 24 hours prior to landing in the United States); and 24-hour Emergency point of contact (e.g., broker, dispatcher, repair shop, or other third party who is knowledgeable about this particular flight); name (first, last, and middle (if available) and telephone number (as applicable).

\1\ As listed in 19 CFR 122.24, if applicable, unless an exemption has been granted under 19 CFR 122.25, or the aircraft was inspected by CBP Officers in the U.S. Virgin Islands.

CBP collects passenger and crewmember information provided by the pilot and/or air, vessel, bus, or rail carrier in advance of passenger and crewmember arrival in or departure from (and, for crew on flights flying over) the United States. CBP maintains this information in APIS. The information is used to perform counterterrorism and/or intelligence activities; to assist law enforcement activities; to perform public security queries that identify risks to the aircraft or vessel, to its occupants; or to the United States and to expedite CBP processing.

Under a previous revision to the APIS rule, (72 FR 48342, published August 23, 2007) CBP mandated pre-departure transmission by air and vessel carriers of personally identifiable information about passengers and crewmembers (including ``non-crew'' as defined in the 2005 APIS Final Rule) traveling by air or sea, arriving in, or departing from (and, in the case of crew, flights overflying) the United States. For more information please see the initial APIS Privacy Impact Assessment (PIA) and Privacy Policy, which was published in the Federal Register (FR), (70 FR 17852, April 7, 2005). Under the most recent Final Rule revision to APIS CBP amended regulations to extend this requirement to private aircraft passengers and crew as well. This information is often collected and maintained on what is referred to as the manifest. The information that CBP requires carriers to collect and submit to APIS (or which may be provided voluntarily by carriers in the rail and bus environments) can be found on routine travel documents that passengers and crewmembers must provide when processed into or out of the United States.

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; who may be a known or suspected terrorist; who may be affiliated with or suspected of being affiliated with terrorists; who may be inadmissible; who may be a person of interest; who may otherwise be engaged in activity in violation of U.S. law; or who may be the subject of wants or warrants. The system allows CBP to effectively and efficiently facilitate the entry and departure of legitimate travelers into and from the United States. DHS officers

can quickly reference the results of the advanced research that has been conducted through CBP's law enforcement databases by using APIS. Results include information from the terrorist screening database (TSDB) and information on individuals with outstanding wants or warrants. These results also confirm the accuracy of that information through comparison with information obtained from the traveler (passenger and crew) and from the carriers, and assists in making 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 one year 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 (BCI), which is a subsystem of the Information Technology platform TECS. Primary inspection lane and ID inspector are added to APIS and the APIS information is verified during physical processing at the border. The information derived from APIS includes (or in the case of rail/bus, may include): Complete name, date of birth, gender, date of arrival, date of departure, time arrived, means of arrival (air/sea/rail/bus), travel document, departure location, airline code, flight number, and the result of the CBP processing. Additionally, a copy of certain APIS data is transferred to the Arrival and Departure Information System (ADIS) for effective and efficient tracking of foreign nationals for individuals subject

[[Page 13409]]

to Office of Biometric Identity Management (OBIM) requirements. This information includes the identification of lawfully admitted non-immigrants who remain in the United States beyond the period of authorized stay. OBIM applies to all visitors (with limited exemptions). The SORN for ADIS was last published on May 28, 2013 (78 FR 31955). 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.

In accordance with the Privacy Act of 1974 and as part of DHS's ongoing effort to review and update legacy system of record notices, DHS/CBP proposes to update and reissue the following system of records notice, DHS/CBP-005 Advance Passenger Information System (APIS) (73 FR 68435, published November 18, 2008), as a DHS/CBP system of records notice titled, DHS/CBP-005 Advance Passenger Information System (APIS) System of Records. DHS/CBP changed the system, changed the security classification to reflect storage of records on a classified network, changed the system location to reflect a new location, updated the purpose to allow for replication of data for analysis and vetting, updated storage due to the change in security classification, updated the retention and disposal to reflect that records will follow the same retention schedule, updated the routine uses to reflect sharing with the news media and public, and changed the notification procedure to reflect that DHS/CBP will now review replicated records.

Consistent with DHS's information sharing mission, information stored in the DHS/CBP-005 APIS System of Records may be shared with other DHS components that have a need to know the information in order to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, information may be shared with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

Additionally, the exemptions for this system of records notice will remain in place. This updated system will be included in the DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate 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 from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

Below is the DHS/CBP-005 Advanced Passenger Information System (APIS) System of Records.

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 Congress.

System of Records

Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-005

System Name:

DHS/CBP-005 Advanced Passenger Information System (APIS).

Security Classification:

Unclassified. The data may be retained on the classified networks but this does not change the nature and character of the data until it

is combined with classified information.

System Location:
Records are maintained in the operational system at CBP Headquarters in Washington, DC and at CBP field offices. Records are replicated from the operational system and maintained on the DHS unclassified and classified networks. This computer database is located at CBP National Data Center (NDC) in Washington, DC. Computer terminals are located at customhouses, border ports of entry, airport inspection facilities under the jurisdiction of DHS, and other locations at which DHS authorized personnel may be posted to facilitate DHS's mission. Terminals may also be located at appropriate facilities for other participating government agencies.

Categories of individuals covered by the system:
Categories of individuals covered by this notice includes passengers who arrive and depart the United States by air, sea, rail, and bus, 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; crew members who arrive and depart the United States by air, sea, rail, and bus, 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 crew members on aircraft that fly over the United States.

Categories of records in the system:
The records in the database include 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 (for all private aircraft passengers and crew, and commercial air, rail, bus, and vessel passengers except for U.S. citizens, lawful permanent residents, crew, and those in transit);
Place of birth and address of permanent residence (commercial flight crew only);
Pilot certificate number and country of issuance (flight crew only, if applicable);
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, air and sea carriers or operators covered by the APIS rules, and rail and bus carriers, to the extent voluntarily applicable, transmit or provide, respectively, 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;

[[Page 13410]]

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;
For passengers and crew members that are transiting through (and crew on flights flying over) 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.
Other information stored in this system of records includes:
Aircraft registration number provided by pilots of private air craft;
Type of aircraft, call sign (if available);
CBP issued decal number (if available);
Place of last departure (ICAO airport code, when available);
Date and time of aircraft arrival;
Estimated time and location of crossing U.S. border/coastline;
Name of intended airport of first landing; \2\

\2\ As listed in 19 CFR 122.24, if applicable, unless an exemption has been granted under 19 CFR 122.25, or the aircraft was inspected by CBP Officers in the U.S. Virgin Islands.

Owner/lessee name (first, last, and middle, if available, or business entity name);

Owner/lessee address (number and street, city, state, zip code, country, telephone number, fax number, and email address, pilot/private aircraft pilot name (last, first, and middle, if available));

Pilot license number, pilot street address (number and street, city, state, zip code, country, telephone number, fax number, and email address);

Pilot license country of issuance, operator name (for individuals: last, first, and middle, if available, or name of business entity, if available);

Operator street address (number and street, city, state, zip code, country, telephone number, fax number, and email address);

Aircraft color(s);

Complete itinerary (foreign airport landings within 24 hours prior to landing in the United States);

24-hour Emergency point of contact (e.g., broker, dispatcher, repair shop, or other third party who is knowledgeable about this particular flight) name (first, last, and middle (if available) and telephone number; and

Incident to the transmission of required information via eAPIS, records will also incorporate the pilot's email address.

Authority for maintenance of the system:

The Aviation and Transportation Security Act of 2001, Pub. L. 107-71; the Enhanced Border Security and Visa Reform Act of 2002, Pub. L. 107-173; the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458; and the Tariff Act of 1930, Pub. L. 71-361, 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, vessel, rail, bus, 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 more effectively and efficiently facilitate 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.

DHS maintains a replica of some or all of the data in the operating system on the unclassified and classified DHS networks to allow for analysis and vetting consistent with the above stated purposes and this published notice.

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 the Department of Justice (DOJ), including Offices of the United States Attorneys or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or 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 any component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity when 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 at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) 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 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.

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. The Department has determined that as a result of the suspected or confirmed compromise, there is a risk of identity theft or fraud, harm to economic or property interests, harm to an individual, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; and

3. The disclosure 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

[[Page 13411]]

agreement, or other assignment for DHS, 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 an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To a federal, state, or local agency, or other appropriate entity or individual, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

I. To a federal, state, tribal, local, or foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence information, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, related rules, regulations, or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

J. To federal and foreign government intelligence or counterterrorism agencies or components when DHS reasonably believes there to be a threat or potential threat to national or international security for which the information may be useful in countering the threat or potential threat, when DHS reasonably believes 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.

K. To an organization or individual in either the public or private sector, either foreign or domestic, when 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.

L. 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.

M. 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.

N. 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.

O. 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.

P. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations when 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.

Q. To the carrier that 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 (including, when applicable, the individual's Electronic System for Travel Authorization (ESTA) status as discussed in the DHS/CBP-009 ESTA SORN (79 FR 65414, published November 3, 2014), or is identified as a ``selectee''.

R. 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:
DHS/CBP stores records in this system electronically in the operational system as well as on the unclassified and classified network or on paper in secure facilities in a locked drawer behind a locked door. DHS/CBP stores records on magnetic disc, tape, digital media, and CD-ROM. 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:
DHS/CBP retrieves data by name or other unique personal identifier from an electronic database.

Safeguards:
DHS/CBP safeguards records in this system 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. In addition, the system manager has the capability to maintain system back-ups for the purpose of supporting continuity of operations and the discrete need to

[[Page 13412]]

isolate and copy specific data access transactions for the purpose of conducting security incident investigations.
All communication links with the CBP data center 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 National Institute of Standards and Technology standards. The last certification was in December 2014.

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 BCI system, a subsystem of TECS. Additionally, for individuals subject to CBP requirements, a copy of certain APIS data is transferred to the ADIS for effective and efficient processing of foreign nationals. More information about ADIS records can be found in the DHS/National Protection and Programs Directorate-001 ADIS SORN (78 FR 31955, published May 28, 2013). Different retention periods apply for APIS data contained in those systems.
Records replicated on the unclassified and classified networks will follow the same retention schedule.

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

Notification procedure:
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 CBP Customer Service Center, OPA, U.S. Customs and Border Protection, 90 K Street NE., Washington, DC 20229 (phone: 877-CBP-5511).
In processing requests for access to information in this system, CBP reviews not only the records in the operational system but also the records that were replicated on the unclassified and classified networks, and provides appropriate access to the information based on this notice.
Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the CBP Freedom of Information Act (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 and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive SW., Building 410, STOP-0655, Washington, DC 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 Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov or 1-866-431-0486. In addition you should:

Explain 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; and

Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

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. In addition, if individuals are uncertain what agency handles the information, they may seek redress through the DHS Traveler Redress Program (TRIP). For more information please see the DHS/ALL-005 DHS Redress and Response System of Records (72 FR 2294, published January 18, 2007). Individuals who believe they have been improperly denied entry, refused boarding for transportation, or identified for additional screening by CBP may submit a redress request through TRIP. TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs such as airports, seaports, and train stations or at U.S. land borders. Travelers can request correction of errors stored in other DHS databases through one application through TRIP. Redress requests should be sent to: DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip.

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 Customer Service Center, OPA, U.S. Customs and Border Protection, 90 K Street NE., Washington, DC 20229 (phone: 877-CBP-5511). If the individual is uncertain what agency is responsible for maintaining the information, redress requests may be sent to DHS TRIP at DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip.

Record source categories:

The system contains data received from private and commercial aircraft pilots, 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 private aircraft, air, or, vessel carriers covered by APIS regulations. The system also contains data to the extent voluntarily submitted by rail and bus carriers regarding passengers and crewmembers who arrive in, and/or depart from the United States. During physical processing at the border, primary inspection lane and ID inspector are added to APIS, and the

[[Page 13413]]

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 that are exempt from certain provision of the Privacy Act. This system may also contain accountings of disclosures made with respect to information maintained in the system. 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: February 27, 2015.

Karen L. Neuman,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2015-05798 Filed 3-12-15; 8:45 am]
BILLING CODE 9111-14-P