Appendix A Update: Data Framework Data Sets

Last updated: February 14, 2018

Appendix A includes details and information on approved datasets in the Data Framework. The information included on the datasets includes: dataset name, description, relevant compliance documents, populations covered, data elements covered, data retention requirements, data refresh rates within the Data Framework, and the date approved to enter Data Framework. As information is updated to these datasets or as datasets are added to the Data Framework this Appendix will be updated accordingly.

The datasets described on the following pages are approved for the Data Framework and their data is currently in the Data Framework. The Data Framework ingests data elements from these datasets. Any future changes to the elements in these datasets will be captured and updated in this Appendix. Other datasets are pending approval for the Data Framework. The Data Framework will ingest data elements from these datasets, pending approval from the Data Framework governance structure, including the oversight offices and each of the dataset stewards. Any future changes to the elements in these datasets will be captured and updated in this Appendix.

This update accounts for the approval of six additional datasets for ingestion into the Data Framework: Border Crossing Information data, Automated Biometric Identification System (IDENT) Asylum data, Aviation Worker data, Airspace Waivers and Flight Authorizations for Certain Aviation Operations (Including DCA) data, Maryland Three Airports (MD-3) data, Private Charter and Twelve Five Program data, and Secure Flight Confirmed Matches data.

Table of Contents

1. Electronic System for Travel Authorization (ESTA)

Component U.S. Customs and Border Protection (CBP)

Status Approved. The ESTA data was approved to enter the Data Framework on September 22, 2014.

Description

ESTA is a web-based system that DHS/Customs and Border Protection (CBP) developed in 2008 to determine the eligibility of aliens to travel by air or sea to the United States under the Visa Waiver Program (VWP) pursuant to Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53, codified at 8 U.S.C. § 1187(a)(11), (h)(3). CBP uses the information submitted to ESTA to make a determination whether the applicant's intended travel poses a law enforcement or security risk.

Relevant Compliance Documents

PIA

DHS/CBP/PIA-007(d) Electronic System for Travel Authorization[1]

Associated SORN(s)

DHS/CBP-009 Electronic System for Travel Authorization (ESTA) System of Records[2]

Individuals Covered

Per the ESTA SORN, categories of individuals covered by this system include:

- Foreign nationals who seek to enter the United States by air or sea under the VWP; and
- Persons, including U.S. citizens and lawful permanent residents, whose information is provided in response to ESTA application questions.

Data Elements Covered

VWP travelers obtain the required travel authorization by electronically submitting an application consisting of biographical and other data elements via the ESTA web site. The categories of records in ESTA include:

[1] DHS/CBP/PIA-007 Electronic System for Travel Authorization and subsequent updates, *available at* www.dhs.gov/privacy.
[2] DHS/CBP-009 Electronic System for Travel Authorization (ESTA) System of Records, 81 FR 60713 (Sept. 2, 2016).

- Full Name (First, Middle, and Last);
- Other names or aliases, if available;
- Date of birth;
- City of birth;
- Gender;
- Email address;
- Telephone number (home, mobile, work, other);
- Home address (address, apartment number, city, state/region);
- IP address;
- ESTA application number;
- Country of residence;
- Passport number;
- Passport issuing country;
- Passport issuance date;
- Passport expiration date;
- Department of Treasury pay.gov payment tracking number (i.e., confirmation of payment; absence of payment confirmation will result in a "not cleared" determination);
- Country of citizenship;
- Other citizenship (country, passport number);
- National identification number, if available;
- Date of anticipated crossing;
- Carrier information (carrier name and flight or vessel number);
- City of embarkation;
- Address while visiting the United States (number, street, city, state);
- Emergency point of contact information (name, telephone number, email address);
- U.S. Point of Contact (name, address, telephone number);

- Parents' names;
- Current job title;
- Current or previous employer name;
- Current or previous employer street address;
- Current or previous employer telephone number; and
- Any change of address while in the United States.

Data Retention Requirements

Application information submitted to ESTA generally expires and is deemed "inactive" two years after the initial submission of information by the applicant. In the event that a traveler's passport remains valid for less than two years from the date of the ESTA approval, the ESTA travel authorization will expire concurrently with the passport. Information in ESTA will be retained for one year after the ESTA travel authorization expires. After this period, the inactive account information will be purged from online access and archived for 12 years. Data linked at any time during the 15-year retention period (generally 3 years active, 12 years archived), to active law enforcement lookout records, will be matched by CBP to enforcement activities, and/or investigations or cases, including ESTA applications that are denied authorization to travel, will remain accessible for the life of the law enforcement activities to which they may become related. NARA guidelines for retention and archiving of data will apply to ESTA and CBP continues to negotiate with NARA for approval of the ESTA data retention and archiving plan. Records replicated on the unclassified and classified networks will follow the same retention schedule.

Payment information is not stored in ESTA, but is forwarded to pay.gov and stored in CBP's financial processing system, Credit/Debit Card Data System (CDCDS), pursuant to the DHS/CBP-018 CDCDS system of records notice.[3]

When a VWP traveler's ESTA data is used for purposes of processing his or her application for admission to the United States, the ESTA data will be used to create a corresponding admission record in the DHS/CBP-016 Nonimmigrant and Immigrant Information System (NIIS).[4] This corresponding admission record will be retained in accordance with the NIIS retention schedule, which is 75 years.

Data Refresh Rates within Data Framework

ESTA data is refreshed on a near real time basis within the Data Framework.

---

[3] DHS/CBP-003 Credit/Debit Card Data System, 76 FR 67755 (Nov. 2, 2011).
[4] DHS/CBP-016 Nonimmigrant and Immigrant Information System, 80 FR 13398 (March 13, 2015).

2. Alien Flight Student Program (AFSP)

Component Transportation Security Administration (TSA)

Status Approved. The AFSP data was approved to enter the Data Framework on September 30, 2014.

Description

The Transportation Security Administration (TSA) conducts Security Threat Assessments (STA) on individuals who are not U.S. citizens or nationals and other individuals designated by TSA seeking flight instruction or recurrent training from Federal Aviation Administration (FAA)-certified flight training providers. The mission of AFSP is to ensure that aliens and other individuals designated by TSA seeking training at flight schools regulated by the FAA do not pose a threat to aviation or national security.

Relevant Compliance Documents

PIA

DHS/TSA/PIA-026 Alien Flight Student Program (AFSP)[5]

Associated SORN(s)

DHS/TSA-002 Transportation Security Threat Assessment System SORN[6]

Individuals Covered

Individuals who undergo a security threat assessment, employment investigation, or other evaluation performed for security purposes, or in order to obtain access to the following: transportation infrastructure or assets, such as terminals, facilities, pipelines, railways, mass transit, vessels, aircraft, or vehicles; restricted airspace; passenger baggage; cargo; shipping venues; or other facilities or critical infrastructure over which DHS exercises authority.

Data Elements Covered

According to the Transportation Security Threat Assessment System SORN, DHS/TSA's system may contain any, or all, of the following information regarding individuals covered by this system:

- Name (including aliases or variations of spelling);
- Gender;

[5] DHS/TSA/PIA-026 Alien Flight Student Program (AFSP), *available at* www.dhs.gov/privacy.
[6] DHS/TSA-002 Transportation Security Threat Assessment System SORN, 79 FR 46862 (Aug. 11, 2014).

- Current and historical contact information (including, but not limited to, address information, telephone number, and email);
- Government-issued licensing or identification information (including, but not limited to, Social Security number (SSN); pilot certificate information, including number and country of issuance;
- Current and past citizenship information; immigration status; alien registration numbers; visa information; and other licensing information for modes of transportation;
- Date and place of birth;
- Name and information, including contact information and identifying number (if any) of the airport, aircraft operator, indirect air carrier, maritime or land transportation operator, or other employer or entity that is employing the individual, or submitting the individual's information, or sponsoring the individual's background check/threat assessment;
- Physical description, fingerprint and/or other biometric identifier, and photograph;
- Date, place, and type of flight training or other instruction;
- Control number or other unique identification number assigned to an individual or credential;
- Information necessary to assist in tracking submissions, payments, and transmission of records;
- Results of any analysis performed for security threat assessments and adjudications;
- Other data as required by Form FD 258 (fingerprint card) or other standard fingerprint cards used by the Federal Government;
- Information provided by individuals covered by this system in support of their application for an appeal or waiver;
- Flight information, including crew status on board;
- Travel document information (including, passport information, including number and country of issuance; and current and past citizenship information and immigration status, any alien registration numbers, and any visa information);
- Criminal history records;

- Data gathered from foreign governments or entities that is necessary to address security concerns in the aviation, maritime, or land transportation systems;
- Other information provided by federal, state, and local government agencies or private entities relevant to the assessment, investigation, or evaluation;
- The individual's level of access at an airport or other transportation facility, including termination or expiration of access;
- Military service history; and
- Suitability testing and results of such testing.

Data Retention Requirements

For individuals not identified as a possible security threat, records will be destroyed one year after DHS/TSA is notified that access based on security threat assessment is no longer valid.

For individuals identified as possible security threats and then subsequently cleared, records will be destroyed seven years after completion of the security threat assessment or one year after being notified that access based on the security threat assessment is no longer valid, whichever is longer.

For an individual that is an actual match to a watchlist, records will be destroyed 99 years after the security threat assessment or seven years after DHS/TSA is notified the individual is deceased, whichever is shorter.

Data Refresh Rates within Data Framework

AFSP data is refreshed on a monthly basis within the Data Framework.

As noted in the Data Framework PIA, to help mitigate the risk due to these non-real-time refreshes, DHS requires users of the Framework to go back to the original DHS IT system and verify that an individual's information has not been updated pursuant to redress or correction before issuing any raw intelligence (e.g., intelligence information report) or final analysis or using the information operationally. Requiring users to verify information in the original DHS IT system will ensure that any updates pursuant to redress or correction will be incorporated into any product or before the information is used operationally.

3. Student Exchange Visitor Information System (SEVIS)

Component U.S. Immigration and Customs Enforcement (ICE)

Status Approved. SEVIS data was approved to enter the Data Framework on October 1, 2014.

Description

SEVIS is a national system to collect and maintain pertinent information on nonimmigrant students and exchange visitors, and the school and exchange visitor sponsors that host these individuals in the United States. Immigration and Customs Enforcement's (ICE) Student and Exchange Visitor Program (SEVP) operates the SEVIS database under the authority of 8 U.S.C. § 1372 in coordination with the Department of State, which oversees the operation of the Exchange Visitor (EV) program.

Relevant Compliance Documents

PIA

DHS/ICE/PIA-001(a) Student Exchange Visitor Information System (SEVIS)[7]

Associated SORN(s)

DHS/ICE-001 Student and Exchange Visitor Information System (SEVIS) System of Records[8]

Individuals Covered

Per the SEVIS SORN, categories of individuals covered by this system include:

- Prospective, current, and former nonimmigrants[9] to the United States on an F-1, M-1, or J-1 class of admission and their dependents who have been admitted under an F-2, M-2, or J-2 class of admission (collectively, F/M/J nonimmigrants);

[7] DHS/ICE/PIA-001(a) Student Exchange Visitor Information System (SEVIS) and subsequent updates, *available at* www.dhs.gov/privacy.
[8] DHS/ICE-001 Student and Exchange Visitor Information System (SEVIS) System of Records, 75 FR 412 (Jan. 5, 2010).
[9] Nonimmigrant classifications are as follows: F nonimmigrants are foreign students pursuing a full course of study in a college, university, seminary, conservatory, academic high school, private elementary school, other academic institution, or language training program in the U.S. that SEVP has certified to enroll foreign students. M nonimmigrants are foreign students pursuing a full course of study in a vocational or other recognized nonacademic institution (e.g., technical school) in the U.S. that SEVP has certified to enroll foreign students. J nonimmigrants are foreign nationals selected by a sponsor that the Department of State (DOS) has designated to participate in an exchange visitor program in the U.S.

- A proxy, parent, or guardian of an F/M/J nonimmigrant; and
- Officials, owners, chief executives, and legal counsel of SEVP-certified schools and designated exchange visitor sponsors.

Data Elements Covered

Biographical information for F/M/J nonimmigrants and school/sponsor officials used in the creation of SEVIS II user account:

- Name(s);
- U.S. domestic address;
- Foreign address (F/M/J nonimmigrants only);
- Date of birth;
- Birth country and city;
- Country of citizenship;
- Country of legal permanent residence;
- Username;
- Email addresses;
- DHS-assigned Immigrant Identification Number (IIN);
- Alien Registration Number (A-Number) (for school/sponsor officials who are U.S. Lawful Permanent Residents only);
- National Identity Number (for F/M/J nonimmigrants only); and
- Passport information (number, issuing country, expiration date).

All of the above information would also be collected for any proxy, parent, or guardian for an F/M/J nonimmigrant who is unable to create his or her own account due to age (under 13 years old), disability, or other reasons. The proxy, parent, or guardian would first need to create his or her own SEVIS II account before he or she could create an account for the F/M/J nonimmigrant.

F-1, M-1, or J-1 nonimmigrant educational and financial information:

- Program of study;
- School registration information;
- Program completion or termination information;

- Transfer information;
- Leave of absence information and study abroad extensions;
- Change of education level;
- Student ID number;
- I-901 fee payment information; and
- Financial information (for F/M nonimmigrants, financial information includes data on source of funds--personal or school, and average annual cost--tuition, books, fees, and living expenses; for J nonimmigrants financial information includes total estimated financial support, financial organization name and support amount).

F/M/J nonimmigrant status and benefit information:

- DHS-assigned Fingerprint Identification Number (for individuals 14 years of age and older);
- U.S. visa number, issuing country, expiration;
- Date;
- Class of admission;
- Immigrant benefit application information (primarily reinstatement, employment authorization, 212e waiver, etc.); and
- Arrival and departure information (port of entry, date of entry/exit).

Data Retention Requirements

Inputs will be deleted after the data has been transferred to the master file and verified. The master file will be retained for 75 years. System outputs are deleted or destroyed when no longer needed for agency business. Once SEVIS II terminates a non-government SEVIS II user account, the system retains user information for 75 years from the date of the last transaction. Government user audit information will be retained for seven years. At this time, SEVP envisions destroying its SEVIS audit records seven years after the date SEVIS II is fully operational. The data from the legacy SEVIS will be retained for seven years.

Data Refresh Rates within Data Framework

SEVIS II data is refreshed on a monthly basis within the Data Framework.

As noted in the Data Framework PIA, to help mitigate the risk due to these non-near real-time refreshes, DHS requires users of the Framework to go back to the original DHS IT system and verify that an individual's information has not been updated pursuant to redress or correction

before issuing any raw intelligence (e.g., intelligence information report) or final analysis or using the information operationally. Requiring users to verify information in the original DHS IT system will ensure that any updates pursuant to redress or correction will be incorporated into any product or before the information is used operationally.

4. Advance Passenger Information System (APIS)

Component U.S. Customs and Border Protection (CBP)

Status Approved. The APIS data was approved to enter the Data Framework on April 22, 2015.

Description

Advance Passenger Information (API) is electronic data collected by DHS from passenger and crew manifest information. Whether collected in conjunction with the arrival or departure of private aircraft, commercial aircraft, or vessels, the purpose of this collection is to identify high risk passengers and crew members who may pose a risk or threat to aircraft or vessel security, national or public security, or who pose a risk of non-compliance with U.S. civil and criminal laws, while simultaneously facilitating the travel of legitimate passengers and crew members. This information collection also assists CBP officers in properly directing resources, resulting in efficient and effective customs and immigration processing at ports of entry.

Relevant Compliance Documents

PIA

DHS/CBP/PIA-001(f) Advance Passenger Information System (APIS)[10]

Associated SORN(s)

DHS/CBP-005 Advance Passenger Information System (APIS) System of Records[11]

Individuals Covered

- 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 over fly the United States.

[10] DHS/CBP/PIA-001(f) Advance Passenger Information System (APIS) *available at* www.dhs.gov/privacy.
[11] DHS/CBP-005 Advance Passenger Information System (APIS) System of Records, 80 FR 13407 (March 15, 2015).

Data Elements Covered

According to the APIS SORN the categories of records in this system are comprised of the following:

- Full Name (First, Middle, and Last);
- 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);
- Passenger Name Record (PNR) locator number;
- Primary inspection lane;
- ID inspector;
- Records containing the results of comparisons of individuals to information maintained in CBP's law enforcement databases;
- Information from the Terrorist Screening Database (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;
- 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 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.

Pilots of private aircraft must provide the following:

- Aircraft registration number;
- 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;
- 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;
- 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, etc.) name (first, last, and middle (if available) and telephone number.

Data Retention Requirements

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 OBIM 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. Different retention periods apply for APIS data contained in those systems.

Data Refresh Rates within Data Framework

APIS data is refreshed every 90 minutes within the Data Framework.

As noted in the Data Framework PIA, to help mitigate the risk due to these non-near real-time refreshes, DHS requires users of the Framework to go back to the original DHS IT system

and verify that an individual's information has not been updated pursuant to redress or correction before issuing any raw intelligence (e.g., intelligence information report) or final analysis or using the information operationally. Requiring users to verify information in the original DHS IT system will ensure that any updates pursuant to redress or correction will be incorporated into any product or before the information is used operationally.

5. Form I-94

Component U.S. Customs and Border Protection (CBP)

Status Approved. The Form I-94 data was approved to enter the Data Framework on April 29, 2015.

Description

CBP issues Form I-94, among other purposes, to provide documentation of the approved length of stay and departure of nonimmigrant aliens. The current form is paper-based and includes a detachable portion with an admission (I-94) number, which the nonimmigrant alien keeps while in the United States as documentation of status.

The forms are scanned and their data elements are manually entered and stored in a file uploaded to CBP's Nonimmigrant and Immigrant Information System (NIIS). In addition, CBP regulations require commercial vessel carriers and commercial and private air carriers to electronically transmit advance manifest information regarding all passengers, crew members, and non-crew members (cargo flights only) arriving and departing the United States via the Advance Passenger Information System (APIS). This information collects similar data as the I-94 form.

Relevant Compliance Documents

PIA

DHS/CBP/PIA-016 I-94 Automation[12]

Associated SORN(s)

DHS/CBP-005 Advanced Passenger Information System (APIS) System of Records[13]

DHS/CBP-016 Nonimmigrant and Immigrant Information System (NIIS) System of Records[14]

Individuals Covered

Per the NIIS SORN, categories of individuals covered by this system are nonimmigrant aliens entering and departing the United States.

Per the APIS SORN, the categories of individuals covered by this system include:

---

[12] DHS/CBP/PIA-016 I-94 Automation *available at* www.dhs.gov/privacy.
[13] DHS/CBP-005 Advanced Passenger Information System (APIS) System of Records, 80 FR 13407 (March 13, 2015).
[14] DHS/CBP-016 Nonimmigrant and Immigrant Information System (NIIS) System of Records, 80 FR 13398 (March 13, 2015).

- 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 over fly the United States.

Data Elements Covered

According to the I-94 PIA, the elements captured on Form I-94 include:

- Family name;
- First (Given) name;
- Birth date;
- Country of citizenship;
- Sex;
- Passport issuance date;
- Passport expiration date;
- Passport number;
- Airline and flight number (if applicable);
- Country where you live;
- Country where you boarded;
- City where visa was issued;
- Date issued;
- Address while in the United States;
- Telephone number in the United States where you can be reached; and
- Email address.

The NIIS SORN covers these data elements, in addition to other data elements related to nonimmigrants.

The APIS SORN covers some of the Form I-94 elements, but could show up under different titles:

- Family name;
- First name;
- Birth date;
- Country of residence;
- Passport number; and
- Address while in the United States.

The APIS SORN also covers additional data elements not related to Form I-94.

Data Retention Requirements

According to the I-94 PIA, the paper-based I-94 document is destroyed after 180 days. The I-94 information collected in NIIS is maintained in NIIS 75 years from the date obtained to inform any future applicable benefits related to immigration and for law enforcement purposes, according to the NIIS SORN. However, if the record is linked to an active law enforcement record and/or investigation that record will remain accessible for the life of the law enforcement activity or investigation.

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 OBIM 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. Different retention periods apply for APIS data contained in those systems.

Data Refresh Rates within Data Framework

I-94 data is refreshed on a daily basis within the Data Framework.

As noted in the Data Framework PIA, to help mitigate the risk due to these non-non-near real-time refreshes, DHS requires users of the Framework to go back to the original DHS IT system and verify that an individual's information has not been updated pursuant to redress or correction before issuing any raw intelligence (e.g., intelligence information report) or final analysis or using the information operationally. Requiring users to verify information in the original DHS IT system will ensure that any updates pursuant to redress or correction will be incorporated into any product

or before the information is used operationally.

6. Passenger Name Record (PNR)

Component U.S. Customs and Border Protection (CBP)

Status Approved. The PNR data was approved to enter the Data Framework on April 22, 2015.

Description

A PNR is a record of travel information created by commercial air carriers that includes a variety of passenger data, such as passenger name, destination, method of payment, flight details, and a summary of communications with airline representatives. PNRs are stored in the Automated Targeting System (ATS) and at the CBP National Targeting Center (NTC). The ATS-Passenger (ATS-P) module facilitates the CBP officer's decision-making about whether a passenger or crew member should receive additional inspection prior to entry into, or departure from, the U.S. because that person may pose a greater risk for terrorism and related crimes.

As a component of ATS, PNR data is covered under the ATS PIA and SORN, which were updated as a result of the European Union and United States PNR Agreement in 2011. All uses of PNR data within the Data Framework will comply with the 2011 Agreement. Please refer to these additional PNR-specific documents for more information:

- U.S. Customs and Border Protection Passenger Name Record (PNR) Privacy Policy;[15]
- *Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security*;[16]
- A Report on the Use and Transfer of Passenger Name Records between the European Union and the United States.[17]

[15] U.S. Customs and Border Protection Passenger Name Record (PNR) Privacy Policy; June 21, 2013, *available at* http://www.cbp.gov/sites/default/files/documents/pnr_privacy.pdf.
[16] *Available at* http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=9382.
[17] A Report on the Use and Transfer of Passenger Name Records between the European Union and the United States; July 3, 2013, *available at* http://www.dhs.gov/sites/default/files/publications/dhs-pnr-privacy-review-20130703.pdf.

Relevant Compliance Documents

PIA

DHS/CBP/PIA-006(d) Automated Targeting System (ATS) – TSA/CBP Common Operating Picture Phase II[18]

Associated SORN(s)

DHS/CBP-006 Automated Targeting System (ATS) System of Records[19]

Individuals Covered

According to the CBP PNR Privacy Policy, a PNR is created for all persons traveling on flights to, from, or through the United States.

The ATS SORN covers this group of individuals, in addition to other categories of individuals related to CBP's targeting mission.

Data Elements Covered

According to the CBP PNR Privacy Policy, the Automated Targeting System-Passenger (ATS-P), a component of ATS, maintains the PNR information obtained from commercial air carriers and uses that information to assess whether there is a risk associated with any travelers seeking to enter, exit, or transit through the United States.

A PNR may include:

- PNR record locator code;
- Date of reservation/issue of ticket;
- Date(s) of intended travel;
- Name(s);
- Available frequent flier and benefit information (i.e., free tickets, upgrades);
- Other names on PNR, including number of travelers on PNR;
- All available contact information (including originator of reservation);
- All available payment/billing information (e.g. credit card number);
- Travel itinerary for specific PNR;

[18] DHS/CBP/PIA-006(d) Automated Targeting System (ATS) – TSA/CBP Common Operating Picture Phase II *available at* www.dhs.gov/privacy.
[19] DHS/CBP-006 Automated Targeting System (ATS) System of Records, 77 FR 30297 (May 22, 2012).

- Travel agency/travel agent;
- Code share information (e.g., when one air carrier sells seats on another air carrier's flight);
- Split/divided information (e.g., when one PNR contains a reference to another PNR);
- Travel status of passenger (including confirmations and check-in status);
- Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote (ATFQ) fields;
- Baggage information;
- Seat information, including seat number;
- General remarks including Other Service Indicated (OSI), Special Service Indicated (SSI) and Supplemental Service Request (SSR) information;
- Any collected APIS information (e.g., Advance Passenger Information (API) that is initially captured by an air carrier within its PNR, such as passport number, date of birth and gender); and
- All historical changes related to the PNR.

Please note that not all air carriers maintain the same sets of information in a PNR, and a particular individual's PNR likely will not include information for all possible categories. In addition, PNR does not routinely include information that could directly indicate the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, or sex life of the individual. To the extent PNR does include terms that reveal such personal matters, an automated system is employed that filters certain terms and only uses this information in exceptional circumstances when the life of an individual could be imperiled or seriously impaired.

The ATS SORN covers these data elements, in addition to other data elements necessary for CBP's targeting mission.

Data Retention Requirements

According to the CBP PNR Privacy Policy, the retention period for data maintained in ATS-P will not exceed fifteen years, after which time it will be deleted. The retention period for PNR, which is contained only in ATS-P, will be subject to the following further access restrictions:

- ATS-P users will have general access to PNR for five years, after which time the PNR data will be moved to dormant, non-operational status;

- After the first six months, the PNR will be "depersonalized," with names, contact information, and other personally identifiable information masked in the record; and
- PNR data in dormant status will be retained for an additional ten years and may be accessed only with prior supervisory approval and only in response to an identifiable case, threat, or risk.

Such limited access and use for older PNR strikes a reasonable balance between protecting this information and allowing CBP to continue to identify potential high-risk travelers.

Information maintained only in ATS-P that is linked to law enforcement lookout records, CBP matches to enforcement activities, investigations, or cases (i.e., specific and credible threats, and flights, individuals and routes of concern, or other defined sets of circumstances), will remain accessible for the life of the law enforcement matter to support that activity and other related enforcement activities.

The ATS SORN allows for longer retention periods from other data sources depending on the retention requirements of those sources.

Data Refresh Rates within Data Framework

PNR data is refreshed on a daily basis within the Data Framework.

As noted in the Data Framework PIA, to help mitigate the risk due to these non-near real-time refreshes, DHS requires users of the Framework to go back to the original DHS IT system and verify that an individual's information has not been updated pursuant to redress or correction before issuing any raw intelligence (e.g., intelligence information report) or final analysis or using the information operationally. Requiring users to verify information in the original DHS IT system will ensure that any updates pursuant to redress or correction will be incorporated into any product or before the information is used operationally.

7. Section 1367 Data Extracted from the Central Index System

Component United States Citizenship and Immigration Services

Status Approved. The Section 1367 data was approved to enter the Data Framework on September 17, 2015.

Description

The Department of Homeland Security United States Citizenship and Immigration Services maintains the Central Index System (CIS), a database system originally developed by the legacy Immigration and Naturalization Service. CIS contains information on the status of 57 million applicants/petitioners seeking immigration benefits to include: lawful permanent residents, naturalized citizens, U.S. border crossers, aliens who illegally entered the U.S., aliens who have been issued employment authorization documents, individuals who petitioned for benefits on behalf of family members, and other individuals subject to the provisions of the Immigration and Nationality Act (INA).

DHS is extracting a subset of CIS data for ingest into the Data Framework. DHS is extracting "Section 1367 data" which is used to identify individuals with special confidentiality protections granted under 8 U.S.C. §1367.

Relevant Compliance Documents

PIA

DHS/USCIS/PIA-009 Central Index System (CIS)[20]

Associated SORN(s)

DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records[21]

Individuals Covered

Any information relating to aliens who are seeking or have been approved for immigrant status as battered spouses, children and parents under provisions of the Violence Against Women Act (VAWA),[22] as victims of a severe form of human trafficking who generally are cooperating

[20] DHS/USCIS/PIA-009 Central Index System (CIS) and subsequent updates, *available at* www.dhs.gov/privacy.
[21] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017).
[22] Public Law 103-322, Violence Against Women Act (VAWA) of 1994; Public Law 106-386, Victims of Trafficking and Violence Protection Act of 2000." (VTVPA); Public Law 109-162, Violence Against Women and

with law enforcement authorities, or as aliens who have suffered substantial physical or mental abuse and are cooperating with law enforcement authorities. This definition includes records or other information that do not specifically identify the individual as an applicant or beneficiary of the T Visa, U Visa, or VAWA protections.

Section 1367 covers information relating to beneficiaries of applications for a number of immigration benefits, not just the Form I-360 VAWA self-petition. If an alien is the beneficiary of a pending or approved application for one or more of the victim-based benefits described below, the requirements of 8 U.S.C. 1367 will be followed:[23]

- VAWA self-petitioner, which incorporates the following applications or petitions:
  - I-360 Self-petition - self-petitioners under INA sec. 204
  - I-751 Hardship waiver - battered spouse or child hardship waiver
  - VAWA CAA - abused Cuban Adjustment Act applicants
  - VAWA HRIFA - abused Haitian Refugee Immigration Fairness Act applicants
  - VAWA NACARA - abused Nicaraguan Adjustment and Central American Relief Act applicants
  - VAWA Suspension of Deportation
- VAWA Cancellation of Removal applicants under INA 240A(b)(2);
- I-914 T Nonimmigrant Status - victim of a severe form of trafficking in persons under INA 101(a)(15)(T); and
- I-918 U Nonimmigrant Status - victim of qualifying criminal activity under INA 101(a)(15)(U).

Data Elements Covered

Section 1367 information is stored within the CIS, which is covered by the A-File SORN. Data elements included with this ingest include:

- Name;

Department of Justice Reauthorization Act of 2005, Section 817 "VAWA Confidentiality Nondisclosure." (VAWA 2005); Public Law 113-4, Violence Against Women Reauthorization Act of 2013, Section 810, "Disclosure of Information for National Security Purposes." (VAWA 2013).

[23] DHS Management Instruction 002-02-001 IMPLEMENTATION OF SECTION 1367 INFORMATION PROVISIONS *available at* http://www.dhs.gov/sites/default/files/publications/implementation-of-section-%201367-%20information-provisions-instruction-002-02-001_0_0.pdf.

- Date of birth;
- Gender;
- Alien Registration Number (A-Number);
- Class of admission;
- Date of entry into status;
- Country of birth;
- Country of citizenship;
- Port of Entry;
- Date file opened;
- Benefit status;
- Passport number;
- Federal Bureau of Investigation (FBI) number; and
- Fingerprint number.

Data Retention Requirements

CIS records are permanently retained.

Data Refresh Rates within Data Framework

Section 1367 data is refreshed on a daily basis within Data Framework.

As noted in the Data Framework PIA, to help mitigate the risk due to these non-near real-time refreshes, DHS requires users of the Framework to go back to the original DHS IT system and verify that an individual's information has not been updated pursuant to redress or correction before issuing any raw intelligence (e.g., intelligence information report) or final analysis or using the information operationally. Requiring users to verify information in the original DHS IT system will ensure that any updates pursuant to redress or correction will be incorporated into any product or before the information is used operationally.

8. Refugee, Asylum and Parole System (RAPS)

Component United States Citizenship and Immigration Services

Status Approved. The RAPS data was approved to enter the Data Framework on December 17, 2015.

Description

The Department of Homeland Security United States Citizenship and Immigration Services maintains the Refugee, Asylum and Parole System (RAPS). RAPS is a comprehensive case management tool that enables USCIS to handle and process applications for asylum pursuant to Section 208 of the Immigration and Naturalization Act (INA) and applications for suspension of deportation or special rule cancellation of removal pursuant to Nicaraguan Adjustment and Central American Relief Act (NACARA) § 203. DHS offices worldwide can access RAPS as a resource of current and historic immigration status information on more than one million applicants. DHS officials can use RAPS to verify the status of asylum applicants, asylees, and their dependents to assist with the verification of an individual's immigration history in the course of a review of visa petitions and other benefit applications as well.

Relevant Compliance Documents

PIA

DHS/USCIS/PIA-27 Refugee, Asylum and Parole System and the Asylum Pre-Screening System[24]

Associated SORN(s)

DHS/USCIS-010 Asylum Information and Pre-Screening System of Records[25]

Individuals Covered

- Individuals covered by provisions of section 208 of the Immigration and Nationality Act (Act), as amended, who have applied with USCIS for asylum on Form I-589 (Application for Asylum and for Withholding of Removal) and/or for suspension of deportation/special rule cancellation of removal under section 203 of NACARA on Form I-881 (Application for Suspension of Deportation or Special Rule Cancellation of Removal);

24 DHS/USCIS/PIA-27 USCIS Asylum Division, *available at* www.dhs.gov/privacy.
25 DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (Nov. 30, 2015).

- The spouse and children of a principal asylum applicant properly included in an asylum application; and
- Persons who complete asylum applications on behalf of the asylum applicant (e.g., attorneys, form preparers, representatives).

Data Elements Covered

Names: USCIS collects names (First, Last, and Middle) and aliases for principal applicants, family members, also known as derivatives, and the preparer of the application in RAPS. Contact information of the attorney or representative is not captured in RAPS as this is available in the Private Attorney Maintenance System (PAMS).

Information Regarding Immigration Status: USCIS collects information relating to immigration status such as A-Numbers, port and date of entry, status at entry, filing date of asylum application, basis of eligibility, interview location, encounter location (i.e., where an Asylum Officer first encounters the individual), immigration court, deportation information, employment authorization eligibility and application history, case status, and case history in certain forms and enters them into RAPS as part of the application process for asylum, NACARA, credible fear and reasonable fear.

Addresses: USCIS collects the addresses of applicants and/or application preparers in RAPS. In addition, USCIS collects this information to substantiate an applicant's claim of continuous residence in the U.S. as required to establish eligibility in some applications.

Telephone Numbers: USCIS collects telephone numbers of the applicant and preparer in order to have a secondary means of contacting either when needed to collect or provide information.

Birth Dates: USCIS collects birth dates (applicant, petitioner, spouse, children/stepchildren/adopted children) and enters them into RAPS.

Social Security Numbers: USCIS collects Social Security numbers (applicant and spouse) and enters them into RAPS.

Citizenship/Nationality/Religion Information: USCIS collects information on the applicant's country of nationality, country of birth, ethnic origin, province of residence in home country, languages spoken, and religion.

Marital Status: USCIS collects information regarding marital status (i.e., whether applicant is married, single, widowed, or divorced) and enters this information into RAPS.

Gender: USCIS collects the genders of the applicant and dependents and enters them into RAPS.

Results of Background Security and Identity Checks: Queries of background and security check systems based on name and date of birth or biometrics return results for newly filed applications and whenever a check is reinitiated to renew an expiring check or prior to a decision. Each check and law enforcement system is briefly summarized below.

- **CBP TECS check** – A check on the applicant's name and date of birth returns a positive or negative response to RAPS. The response will be displayed in RAPS as a positive or negative match. This check can be renewed manually.
- **ENFORCE Alien Removal Module (EARM) check** – A check on the applicant's name and date of birth returns a positive or negative response to RAPS. The response will be displayed in RAPS as a positive or negative match. This check can take place through the automated interface one time only.
- **FBI Fingerprint check** – A check on the applicant's ten-print biometrics returns the date of the applicant's fingerprint appointment at an USCIS Application Support Center (ASC), the date that the biometrics are sent to the FBI, and the date and the result of the check. The response will be displayed in RAPS as a positive or negative match. This check can be renewed manually via RAPS.
- **FBI Name check** – A check on all names and dates of birth used by the applicant return a positive or negative response to RAPS. The response will be displayed in RAPS as a positive or negative match for each alias and alternate date of birth.
- **US-VISIT/IDENT check** – A check on the applicant's ten-print biometrics returns the applicant's identification number assigned by US-VISIT/IDENT, the dates that the information is collected and uploaded to the system, and the nature of the hit (whether the hit is of a law enforcement nature), if any. New information uploaded to US-VISIT/IDENT will appear in the applicant's system record if it is of a higher law enforcement interest than prior hits.

Background and security check results are uploaded to RAPS during a nightly update. The results of checks are also included on reports automatically generated at each Asylum Office listing individuals flagged as potential "hits." Most security checks expire or are limited in verification for a specific application; therefore, RAPS allows checks to be reinitiated as necessary. It should be noted that RAPS does not contain all information provided in the I-589 or I-881, such as descriptive narratives related to the basis of the claim and information on the applicant's educational background and past addresses. Also, no biometric data or photographs are stored in RAPS.

Preparers: Data on individuals who prepared the asylum application are collected in RAPS.

Relatives: Spousal and parent-child relationships are collected. In RAPS NACARA § 203 cases, relationship information may be entered to support the applicant's eligibility.

Data Retention Requirements

The A-File records are permanent whether hard copy or electronic. USCIS transfers the A-Files to the custody of NARA 100 years after the individual's date of birth: RAPS Master File automated records are maintained for 25 years after the case is closed and then destroyed. Information in the master file is destroyed 15 years after the last completed action with respect to the benefit.

Data Refresh Rates within Data Framework

RAPS data is refreshed on a daily basis within Data Framework.

As noted in the Data Framework PIA, to help mitigate the risk due to these non-near real-time refreshes, DHS requires users of the Framework to go back to the original DHS IT system and verify that an individual's information has not been updated pursuant to redress or correction before issuing any raw intelligence (e.g., intelligence information report) or final analysis or using the information operationally. Requiring users to verify information in the original DHS IT system will ensure that any updates pursuant to redress or correction will be incorporated into any product or before the information is used operationally.

9. Ship Arrival Notification System (SANS)

Component United States Coast Guard

Status Approved. The SANS data was approved to enter the Data Framework on December 17, 2015.

Description

The United States Coast Guard (USCG) stores Notice of Arrival and Departure (NOAD) information electronically in the SANS. The U.S. Coast Guard collects NOA information in order to provide for the safety and security of U.S. ports and waterways and the overall security of the United States. This information allows the USCG to facilitate effectively and efficiently the entry and departure of vessels into and from the United States and assist the USCG with assigning priorities while conducting maritime safety and security missions in accordance with international and domestic regulations. PII concerning vessel owner, crew members and/or non-crew individuals is collected to give an accurate picture of who has overall responsibility for a given vessel and who is onboard that vessel. The information is collected for the purpose of ensuring the safety and security of U.S. ports and waterways and the overall security of the United States. It is used to conduct necessary screening and national security checks.

Relevant Compliance Documents

PIA

DHS/USCG/PIA-006(b) Vessel Requirements for the Notice of Arrival and Departure (NOAD) and Automatic Identification System (AIS) Rulemaking[26]

Associated SORN(s)

DHS/USCG-029 Notice of Arrival and Departure System of Records[27]

DHS/USCG-061 Maritime Awareness Global Network (MAGNET) System of Records[28]

Individuals Covered

Crew members who arrive and depart the U.S. by sea and individuals associated with a vessel and whose information is submitted as part of a notice of arrival or notice of departure, including but not limited to vessel owners, operators, charterers, reporting parties, 24-hour contacts, company security officers, and persons in addition to crew who arrive and depart the U.S.

[26] DHS/USCG/PIA-006(b) Vessel Requirements for the Notice of Arrival and Departure (NOAD) and Automatic Identification System (AIS) Rulemaking, *available at* www.dhs.gov/privacy.
[27] DHS/USCG-029 Notice of Arrival and Departure System of Records, 82 FR 32715 (July 17, 2017).
[28] DHS/USCG-061 Maritime Awareness Global Network (MAGNET), 73 FR 28143 (May 15, 2008).

by sea.

Data Elements Covered

USCG collects information from vessels' owners, operators, masters, agents or person in charge of the vessel(s). Information is submitted at 96-hours prior to a vessel's arrival to the United States.

Notice of arrival information collected falls into the following broad categories: Vessel and Voyage Details (including arrival/departure), Crew Information, Non-Crew Information, and Cargo Information.

Specifically, the following information is collected:

Vessel and Voyage Information:

- Name of vessel;
- Name of registered owner;
- Country of registry;
- Call sign;
- International Maritime Organization (IMO) international number or, if vessel does not have an assigned IMO international number, substitute with official number;
- Name of the operator;
- Name of charterer;
- Name of classification society;
- Maritime Mobile Service Identity (MMSI); and
- Vessel(s) gross tonnage.

Voyage Information:

- Arrival information:
    - Names of last five foreign ports or places visited;
    - Dates of arrival and departure for last five foreign ports or places visited;
    - For each port or place of the United States to be visited, a list of the names of the receiving facility, the port or place, the city, and the state;
    - For each port or port or place of the United States to be visited, the estimated date and time of arrival;

- For each port or port or place in the United States to be visited, the estimated date and time of departure;
- The location (port or place and country) or position (latitude and longitude or waterway and mile marker) of the vessel at the time of reporting;
- The name and telephone number of a 24-hour point of contact;
- Duration of the voyage;
- Last five ports of call;
- Dates of arrival and departure in last port or place visited; and
- Estimated date and time of arrival to the entrance of port, if applicable.

- Departure information:
  - The name of departing port or place of the United States, the estimated date and time of departure;
  - Next port or place of call (including foreign), the estimated date and time of arrival; and
  - The name and telephone number of a 24-hour point of contact.

Information for each crewmember onboard:

- Full name;
- Date of birth;
- Nationality;
- Identification information (type, number, issuing country, issue date, expiration date);
- Position or duties on the vessel;
- Where the crewmember embarked (list port or place and country); and
- Where the crewmember will disembark.

Information for each person onboard in addition to crew:

- Full name;
- Date of birth;
- Nationality;

- Identification information (type, number, issuing country, issue date, expiration date);
- U.S. address information;
- Where the person embarked (list port or place and country); and
- Where the person will disembark.

Cargo Information:

- A general description of cargo, other than CDC (certain dangerous cargo), onboard the vessel (e.g., grain, container, oil);
- Name of each certain dangerous cargo carried, including United Nations (UN) number, if applicable;
- Amount of each certain dangerous cargo carried;
- Operational condition of equipment required by 164.35 of this chapter of the International Safety Management (ISM) Code Notice;
- The date of issuance for the company's Document of Compliance certificate;
- The date of issuance of the vessel's Safety Management Certificate;
- The name of the Flag Administration, or recognized organization(s) representing the vessel flag administration, that issued those certificates International Ship and Port Facility Security Code (ISPS) Notice;
- The date of issuance for the vessels international Ship Security Certificate (ISSC), if any;
- Whether the ISSC, if any, is an initial interim ISSC, subsequent and consecutive interim ISSC, or final ISSC;
- Declaration that the approved ship security plan, if any, is being implemented;
- If a subsequent and consecutive interim ISSC, the reasons therefore;
- The name and 24-hour contact information for the Company's Security Officer; and
- The name of the Flag Administration, or recognized security organization(s) representing the vessel flag administration, that issued the ISSC.

Data Retention Requirements

In accordance with NARA Disposition Authority number N1-026-05-11, NOAD

information on vessels and individuals maintained in the SANS is destroyed or deleted when no longer needed for reference, or after ten years, whichever is later. Outputs, which include ad-hoc reports generated for local and immediate use to provide a variety of interested parties, for example, Captain of the Port and marine safety offices, sea marshals, Customs and Border Patrol, Immigration and Customs Enforcement with the necessary information to set up security zones, scheduling boarding and inspections activities, actions for non-compliance with regulations, and other activities in support of USCG's mission to provide for safety and security of U.S. ports, are deleted after five years if they do not constitute a permanent record according to NARA.

Data Refresh Rates within Data Framework

SANS data is refreshed on a near real time basis within Data Framework.

10. Border Crossing Information (BCI)

Component U.S. Customs and Border Protection (CBP)

Status Approved. The BCI data was approved to enter the Data Framework on April 14, 2016 and an update was approved July 21, 2016.

Description

CBP collects and maintains records on border crossing information for all individuals who enter, are admitted or paroled into, and (when available) exit from the United States, regardless of method or conveyance. Border crossing information includes certain biographic and biometric information; photographs; certain mandatory or voluntary itinerary information provided by air, sea, bus, and rail carriers or any other forms of passenger transportation; and the time and location of the border crossing.

Relevant Compliance Documents

PIAs

DHS/CBP/PIA-004(g) Beyond the Border Entry/Exit Program Phase II[29]

DHS/CBP/PIA-008 Border Searches of Electronic Devices[30]

Associated SORN(s)

DHS/CBP-007 Border Crossing Information System of Records[31]

Individuals Covered

Individuals with records stored in BCI include U.S. citizens, lawful permanent residents (LPR), and immigrant and nonimmigrant aliens who lawfully cross the U.S. border by air, land, or sea, regardless of method of transportation or conveyance.

Data Elements Covered

CBP collects and stores the following records in the BCI system as border crossing information:

- Full name (last, first, and, if available, middle);
- Date of birth;
- Gender;

[29] DHS/CBP/PIA-004(g) Beyond the Border Entry/Exit Program Phase II, *available at* www.dhs.gov/privacy.
[30] DHS/CBP/PIA-008 Border Searches of Electronic Devices, *available at* www.dhs.gov/privacy.
[31] DHS/CBP-007 Border Crossing Information System of Records, 81 FR 4040 (Dec. 13, 2016).

- Travel document type and number (e.g., passport information, permanent resident card, Trusted Traveler Program card);
- Issuing country or entity and expiration date;
- Photograph (when available);
- Country of citizenship;
- Tattoos;
- Scars;
- Marks;
- Palm prints;
- Digital fingerprints;
- Photographs;
- Digital iris scans;
- Radio Frequency Identification (RFID) tag number(s) (if land or sea border crossing);
- Date and time of crossing;
- Lane for clearance processing;
- Location of crossing;
- Secondary Examination Status; and
- For land border crossings only, License Plate number or Vehicle Identification Number (VIN) (if no plate exists).

CBP maintains in BCI information derived from an associated Advance Passenger Information System (APIS) transmission (when applicable), including:

- Full name (last, first, and, if available, middle);
- 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, LPRs, 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);
- Passenger Name Record (PNR) locator number;
- Primary inspection lane;
- ID inspector;
- Records containing the results of comparisons of individuals to information maintained in CBP's law enforcement databases as well as information from the Terrorist Screening Database (TSDB);
- Information on individuals with outstanding wants or warrants; and
- Information from other government agencies regarding high risk parties.

CBP collects records under the Entry/Exit Program with Canada, such as border crossing data from the Canada Border Services Agency (CBSA), including:

- Full name (last, first, and if available, middle);
- Date of Birth;
- Nationality (citizenship);
- Gender;
- Document Type;
- Document Number;
- Document Country of Issuance;
- Port of entry location (Port code);
- Date of entry; and
- Time of entry.

In addition, air and sea carriers or operators covered by the APIS rules and rail and bus carriers (to the extent voluntarily applicable) also transmit or provide the following information to CBP for retention in BCI:

- 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.
- For passengers and crew members who 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).
- For passengers and crew departing the United States:
    - Final foreign airport/port of arrival.

Other information also stored in this system of records includes:

- Aircraft registration number provided by pilots of private aircraft;
- Type of aircraft;
- Call sign (if available);
- CBP issued decal number (if available);
- Place of last departure (e.g., ICAO airport code, when available);
- Date and time of aircraft arrival;

- Estimated time and location of crossing U.S. border or coastline;
- Name of intended airport of first landing, if applicable;
- Owner or lessee name (first, last, and middle, if available, or business entity name);
- Owner or lessee contact information (address, city, state, zip code, country, telephone number, fax number, and email address, pilot, or private aircraft pilot name);
- Pilot information (license number, 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 information (e.g., broker, dispatcher, repair shop, or other third party who is knowledgeable about this particular flight):
    - Full name (last, first, and middle (if available)) and telephone number;
- Incident to the transmission of required information via eAPIS (for general aviation itineraries, pilot, and passenger manifests), records will also incorporate the pilot's email address.

To the extent private aircraft operators and carriers operating in the land border environment may transmit APIS, similar information may also be recorded in BCI by CBP with regard to such travel. CBP also collects the license plate number of the conveyance (or VIN number when no plate exists) in the land border environment for both arrival and departure (when departure information is available).

Data Retention Requirements

DHS/CBP is working with NARA to develop the appropriate retention schedule based on the information below. For persons DHS/CBP determines to be U.S. citizens and LPRs, information in BCI that is related to a particular border crossing is maintained for 15 years from

the date when the traveler entered, was admitted to or paroled into, or departed the United States, at which time it is deleted from BCI. For nonimmigrant aliens, the information will be maintained for 75 years from the date of admission or parole into or departure from the United States in order to ensure that the information related to a particular border crossing is available for providing any applicable benefits related to immigration or for other law enforcement purposes.

Information related to border crossings prior to a change in status will follow the 75 year retention period for nonimmigrant aliens who become U.S. citizens or LPRs following a border crossing that leads to the creation of a record in BCI. All information regarding border crossing by such persons following their change in status will follow the 15 year retention period applicable to U.S. citizens and LPRs. For all travelers, however, BCI records linked to active law enforcement lookout records, DHS/CBP matches to enforcement activities, or investigations or cases remain accessible for the life of the primary records of the law enforcement activities to which the BCI records may relate, to the extent retention for such purposes exceeds the normal retention period for such data in BCI.

Records replicated on the unclassified and classified networks for analysis and vetting will follow the same retention schedule.

Data Refresh Rates within Data Framework

BCI data is refreshed every few hours within Data Framework.

11. Automated Biometric Identification System (IDENT) Asylum Data

Components U.S. Citizenship and Immigration Service (USCIS)

National Protection and Programs Directorate (NPPD)

Status Approved. The IDENT Asylum data was approved to enter the Data Framework on June 30, 2016.

Description

NPPD is the system owner for the IDENT system. IDENT is the central DHS-wide system for the storage and processing of biometric and associated biographic information for the purposes of national security, law enforcement, immigration and border management, intelligence, and credentialing (e.g., background investigations for national security positions and certain positions of public trust), as well as for providing associated testing, training, management reporting, planning and analysis, or other administrative uses. Data Framework will ingest certain core biographic IDENT Asylum data. The ingested IDENT Asylum data is data within the IDENT Asylum – Organization, Unit, Subunit (ASY-OUS) data feed. The source system for the ASY-OUS data feed to be ingested is the USCIS Refugee, Asylum and Parole System (RAPS). The Department approved ingestion of the underlying RAPS data into Data Framework on December 17, 2015. In addition, the IDENT ASY-OUS data includes Fingerprint Identification Numbers (FIN) and encounter identification numbers (EID) generated within the IDENT system. The DHS Data Framework will not ingest the entire IDENT ASY-OUS data feed. Rather, ingestion will be limited to the core biographic information, A Number, FIN and EID data, described below.

Relevant Compliance Documents

PIA

DHS/USCIS/PIA-27 Refugee, Asylum and Parole System and the Asylum Pre-Screening System[32]

Associated SORN(s)

DHS/USCIS-010 Asylum Information and Pre-Screening System of Records[33]

Individuals Covered

32 DHS/USCIS/PIA-27 USCIS Asylum Division, available at www.dhs.gov/privacy.
33 DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (Nov. 30, 2015).

- Individuals covered by provisions of section 208 of the Immigration and Nationality Act (Act), as amended, who have applied with USCIS for asylum on Form I-589 (Application for Asylum and for Withholding of Removal) and/or for suspension of deportation/special rule cancellation of removal under section 203 of NACARA on Form I-881 (Application for Suspension of Deportation or Special Rule Cancellation of Removal);
- The spouse and children of a principal asylum applicant properly included in an asylum application; and
- Persons who complete asylum applications on behalf of the asylum applicant (e.g., attorneys, form preparers, representatives).

Data Elements Covered

- Name;
- Date of Birth;
- Gender;
- A-Number;
- Fingerprint Identification Number (FIN) – The FIN uniquely identifies each person in the IDENT database; and
- Encounter Identification Number (EID) – The EID uniquely identifies each virtual or physical encounter.

Data Retention Requirements

The A-File records are permanent whether hard copy or electronic. USCIS transfers the A-Files to the custody of NARA 100 years after the individual's date of birth: RAPS Master File automated records are maintained for 25 years after the case is closed and then destroyed. Information in the master file is destroyed 15 years after the last completed action with respect to the benefit.

Data Refresh Rates within Data Framework

IDENT Asylum data is refreshed daily within Data Framework.

12. Aviation Worker Data

Components Transportation Security Administration

Status Approved. Aviation Worker data was approved to enter the Data Framework on, July 7, 2016.

Description

TSA collects biographic information from individuals to conduct name-based Security Threat Assessments (STAs) of persons seeking airport badges or credentials (Aviation Workers) to identify potential or actual threats to transportation or national security. The STA involves recurring checks against Federal terrorist, immigration, and law enforcement databases. In addition, individuals seeking credentials authorizing unescorted access to sterile areas, secured areas, Air Operations Areas (AOAs), and Security Identification Display Areas (SIDA) must submit their fingerprints to the sponsoring airport or aircraft operator who, in turn, sends this information to their service provider to aggregate the fingerprint data and convert any paper fingerprint cards into an electronic format. The service provider then sends the information via secure email to TSA. TSA sends the fingerprint information to the Federal Bureau of investigation (FBI) to conduct a fingerprint-based Criminal History Record Check (CHRC). Adjudication of the CHRC is conducted by the airport. TSA will also transmit these already collected fingerprints to Office of Biometric Identity Management to perform checks against immigration, terrorism and law enforcement databases held in IDENT. Additionally, TSA requires STAs for certain individuals with airport approved badges. Fingerprint-based checks will be conducted for those individuals whose airport approved badge involves access to the sterile area, secure area, or SIDA.

Relevant Compliance Documents

PIA

DHS/TSA/PIA-020 Security Threat Assessment for Airport Badge and Credential Holders (SIDA)[34]

Associated SORN(s)

DHS/TSA-002 Transportation Security Threat Assessment System[35]

Individuals Covered

Individuals who have "unescorted access" to the secure areas of airports and aircraft.

[34] DHS/TSA/PIA-020 Security Threat Assessment for Airport Badge and Credential Holders (SIDA), *available at* www.dhs.gov/privacy.
[35] DHS/TSA-002 Transportation Security Threat Assessment System, 79 FR 46862 (Aug. 11, 2014).

Data Elements Covered

Full name (last, first, middle as appearing on government-issued ID), other names used, gender, date of birth, place of birth, Social Security Number (SSN), home address, phone number, submitting entity (i.e., employer or prospective employer), fingerprints, citizenship, and, if applicable, passport number and country of issuance, alien registration number or Form I-94 Arrival/Departure Number, or certificate of naturalization number or certificate of birth abroad. In addition, individuals who must submit fingerprints will also provide race, height, weight, eye color, and hair color. TSA will also collect the results of STA. In addition, the system may also include information originating from the terrorism, immigration, or law enforcement databases queried as part of the STA, such as IDENT checks.

Data Retention Requirements

TSA will retain the information in accordance with the National Archives and Records Administration (NARA) records schedule approved March 8, 2007, Transportation Threat Assessment and Credentialing. The approved NARA schedule contains the following dispositions:

- TSA will delete/destroy information contained in the Subject Database System one year after an individual's credential or access privilege granted based upon the STA is no longer valid. In addition, for those individuals who may originally have appeared to be a match to a government watch list, but are subsequently cleared as not posing a threat to transportation or national security, retained information will be deleted/destroyed seven years after completion of the STA, or one year after any credential or access privilege granted based on the STA is no longer valid, whichever is longer.
- Information contained in the Subject Database System on individuals that are actual matches to a government watch list or otherwise pose a threat to transportation or national security, will be deleted/destroyed ninety-nine years after completion of the STA, or seven years after TSA learns that the individual is deceased, whichever is shorter.

Data Refresh Rates within Data Framework

Aviation Worker data is refreshed on a near real-time basis within Data Framework.

13. Airspace Waivers and Flight Authorizations for Certain Aviation Operations (Including DCA) Data

Components Transportation Security Administration (TSA)

Status Approved. The Airspace Waivers and Flight Authorizations for Certain Aviation Operations (Including DCA) data was approved to enter the Data Framework on July 7, 2016.

Description

TSA collects information in order to issue flight authorizations for certain operations into and out of Ronald Reagan National Airport (DCA) (DCA Flight Authorization Program data). TSA authorizes these operations at DCA provided that aircraft operators comply with certain security procedures. These procedures are: Each aircraft operator and each fixed base operator that supports the operation must have appointed a security coordinator. For each flight into and out of DCA the aircraft operator must carry an armed security officer. Each security coordinator, armed security officer, flight crewmember, and all passengers must have been vetted by TSA by undergoing a security threat assessment (STA).

Relevant Compliance Documents

PIA

DHS/TSA/PIA-003 Airspace Waiver and Flight Authorizations for Certain Aviation Operations (Including DCA)[36]

Associated SORN(s)

DHS/TSA-002 Transportation Security Threat Assessment System[37]

Individuals Covered

Flight crewmembers and Passengers who will be onboard the aircraft while it is operating in restricted airspace, Designated Security Coordinators, and Armed Security Officers.

Data Elements Covered

For airspace waivers, through aircraft operators, TSA collects and retains personal information that is used to conduct a security threat assessment on the flight crewmembers and passengers who will be onboard the aircraft while it is operating in restricted airspace. This

[36] DHS/TSA/PIA-003 Airspace Waiver and Flight Authorizations for Certain Aviation Operations (Including DCA), *available at* www.dhs.gov/privacy.
[37] DHS/TSA-002 Transportation Security Threat Assessment System, 79 FR 46862 (Aug. 11, 2014).

information includes: (1) first name, (2) last name, (3) middle name (if applicable), (4) social security number (submission is voluntary, although recommended), (5) passport number (if applicable), (6) passport country of issuance (if applicable), (7) date of birth, and (8) place of birth. Although provision of one's social security number is voluntary, failure to provide a social security number may result in delays in processing the waiver application.

Special procedures apply for aircraft operators seeking flight authorizations for operations into or out of DCA. Under this program, aircraft operators and fixed base operators will be required to designate a security coordinator who is responsible for implementing the applicable security measures as outlined in the rule (See 49 C.F.R. Subpart 1562 Subpart B). TSA will collect fingerprints and the following information to conduct a fingerprint-based criminal history record check and a security threat assessment on the security coordinator: (1) first, middle, and last name, any applicable suffix, and any other names used; (2) current mailing address, including residential address if different than current mailing address; (3) date and place of birth; (4) social security number (submission is voluntary, although recommended); (5) citizenship status and date of naturalization (if applicable); and (6) alien registration number (if applicable). Although provision of one's social security number is voluntary, failure to provide a social security number may result in delays in processing the security threat assessment. TSA also will collect fingerprints and the information listed above from each flight crewmember and armed security officer who will be on board any aircraft operated under a flight authorization into or out of DCA. Finally, TSA will collect the information listed above, but not fingerprints, from each passenger who is not an armed security officer but who will be on board any affected aircraft operations into or out of DCA.

For individuals serving as armed security officers onboard flights into and out of DCA, additional information will be collected including address, citizenship, employment history, personal history, education and training, experience including sworn law enforcement and military experience, and references. This information will be used to verify the individual's qualifications to perform the duties required of armed security officers onboard flights into and out of DCA.

Data Retention Requirements

TSA will delete/destroy the individual's information one (1) year after TSA is notified that an individual's privilege granted based upon the STA/CHRC is no longer valid. In addition, information for those individuals who may originally have appeared to be a match to a government watch list, but are subsequently cleared as not posing a threat to transportation or national security, will be deleted/destroyed seven (7) years after completion of the STA/CHRC, or one (1) year after any privilege granted based on the STA/CHRC is no longer valid, whichever is longer. Information on individuals that are actual matches to a government watch list or otherwise pose a threat to transportation or national security will be deleted/destroyed ninety-nine (99) years after completion of the STA/CHRC, or seven (7) years after TSA learns that the individual is deceased,

whichever is shorter. TSA retains the data IAW National Archives and Records Administration records schedule approved March 8, 2007.

Data Refresh Rates within Data Framework

Airspace Waivers and Flight Authorizations for Certain Aviation Operations (Including DCA) data is refreshed on a near real-time basis within Data Framework.

14. Maryland-Three (MD-3) Airports Data

Components Transportation Security Administration (TSA)

Status Approved. MD-3 Airports data was approved to enter the Data Framework on July 7, 2016.

Description

TSA conducts name-based Security Threat Assessments (STA) and fingerprint-based Criminal History Records Checks (CHRCs) on pilots who operate aircraft and apply for privileges to fly to or from the three General Aviation airports in the Washington, D.C. restricted flight zones (Potomac Airfield, Washington Executive/Hyde Field, and College Park Airport), otherwise known as the Maryland Three (MD-3) program, and for the Airport Security Coordinator (ASC)1 at a MD-3 airport. For the STA process, TSA compares the biographical information of these pilots and ASCs, hereafter referred to as individuals, against Federal terrorist, immigration, and law enforcement databases. For the CHRC, TSA forwards the fingerprints to the Federal Bureau of Investigation (FBI), which conducts fingerprint-based CHRCs on individuals.

Relevant Compliance Documents

PIA

DHS/TSA/PIA-022 Maryland Three (MD-3) Airports[38]

Associated SORN(s)

DHS/TSA-002 Transportation Security Threat Assessment System[39]

Individuals Covered

Individuals who apply for privileges to fly to or from the three General Aviation airports in the Washington, D.C. restricted flight zones as part of the MD-3 program, and for the Airport Security Coordinator at a MD-3 airport in accordance with 49 C.F.R. 1562.3.

Data Elements Covered

Full name (last, first, middle as appearing on a government-issued ID), alias(es), date of birth, Social Security Number (SSN) (voluntary but failure to provide may delay or prevent completion of the STA), home address, phone number, submitting entity (i.e., employer, pilot), fingerprints, and, if applicable, pilot's airmen certificate or student pilot certificate, and pilot's current medical certificate.

[38] DHS/TSA/PIA-022 Maryland Three (MD-3) Airports, *available at* www.dhs.gov/privacy.
[39] DHS/TSA-002 Transportation Security Threat Assessment System, 79 FR 46862 (Aug. 11, 2014).

TSA collects the information from the individuals through private sector service providers, and also collects the results of the STA and CHRC from agencies queried as part of the STA and CHRC.

Data Retention Requirements

TSA will retain the data in accordance with the National Archives and Records Administration (NARA) records schedule approved March 8, 2007. The approved NARA schedule contains the following dispositions:

TSA will delete/destroy the individual's information one year after TSA is notified that an individual's privilege granted based upon the STA/CHRC is no longer valid. In addition, information for those individuals who may originally have appeared to be a match to a government watch list, but are subsequently cleared as not posing a threat to transportation or national security, will be deleted/destroyed seven years after completion of the STA/CHRC, or one year after any privilege granted based on the STA/CHRC is no longer valid, whichever is longer.

Information on individuals that are actual matches to a government watch list or otherwise pose a threat to transportation or national security will be deleted/destroyed ninety-nine years after completion of the STA/CHRC, or seven years after TSA learns that the individual is deceased, whichever is shorter.

Data Refresh Rates within Data Framework

MD-3 Airports data is refreshed on a near real-time basis within Data Framework.

15. Private Charter and Twelve Five Program Data

Components Transportation Security Administration (TSA)

Status Approved. Private Charter and Twelve Five Program data was approved to enter the Data Framework on July 7, 2016.

Description

TSA published a Notice of Proposed Rulemaking (NPRM) to amend aviation transportation security regulations to expand the scope of general aviation requirements and add new requirements for large aircraft operators and airports that service these aircraft. The proposed regulation would have established a security program called the Large Aircraft Security Program (LASP) for the large aircraft operators, and would have required security threat assessments (STAs) for various categories of individuals. No Final Rule was published, but TSA has accepted personally identifiable information to conduct STAs on a voluntary basis for individuals described in the NPRM for operations of aircraft with a maximum certificated takeoff weight above 12,500 pounds, including corporate and private aircraft (Twelve-Five Standard Security Program). In addition, TSA has performed STAs on some individuals described in the LASP NPRM for Private Charter operations where the individual may also be covered by another regulation requiring an STA.

Relevant Compliance Documents

PIA

DHS/TSA/PIA-017 Large Aircraft Security Program[40]

Associated SORN(s)

DHS/TSA-002 Transportation Security Threat Assessment System[41]

Individuals Covered

Passengers, Aircraft Operators, Flight crew member, Auditors, Watch List Service Provider Covered Personnel, and Screeners.

Data Elements Covered

Passenger information: Under the NPRM, aircraft operators would be required to submit passenger full name to an approved Watch List Service Provider for watch list matching purposes. Passenger information will not be provided to TSA unless there is a possible match to the watch

[40] DHS/TSA/PIA-017 Large Aircraft Security Program, *available at* www.dhs.gov/privacy.
[41] DHS/TSA-002 Transportation Security Threat Assessment System, 79 FR 46862 (Aug. 11, 2014).

list. Aircraft operators would request, but not require, submission of passenger gender, date of birth, and TSA Redress Number (if applicable) to assist in eliminating misidentification.

Although TSA would not require large aircraft operators to request passport information from passengers, the proposed rule would require large aircraft operators to transmit certain information from an individual's passport (full name, passport number, country of issuance, expiration date, gender, and date of birth), if it is available and was provided to the aircraft operator. Aircraft operators will transmit the full name and other available passenger information after verifying the information with a government issued identification card. Passengers who frequently fly with the aircraft operator may request to be placed on a Master Passenger List that will be continuously vetted by the Watch List Service Provider.

*Aircraft Operators***:** Aircraft operators required to have a security program under the LASP must submit the following information for purposes of administering the program and communicating with responsible personnel, and conducting a STA and/or checks confirming whether the operators are legitimate business entities and whether their owners are individuals who appear to pose a risk to aviation security:

- Business name to include "doing business as" business names, state of incorporation if applicable and tax identification number;
- Address of primary place of business or headquarters;
- Name and address of each proprietor, general partner, officer, director, and owner;
- FAA operating certificate number of the applicant, if applicable; and
- For contact purposes, the name, title, business address, business telephone number(s) and business electronic mail address of the Aircraft Operator Security Coordinator (AOSC) and any alternates.

*Flight Crew, Auditors, Watch List Service Provider Covered Personnel, and Screeners***:** These individuals must submit the information below for purposes of conducting a security threat assessment:

- Legal name, including first, middle, and last: any applicable suffix, and any other named used previously;
- Current mailing address and residential address if it differs from the mailing address; and the previous residential address;
- Date of birth;
- Social security number (Voluntary but failure to provide it may delay or prevent completion of the threat assessment);

- Gender;
- Height, weight, hair and eye color;
- City, state, and country of birth;
- Immigration status and date of naturalization if the individual is a naturalized citizen of the United States;
- Alien registration number, if applicable;
- The name, telephone number, and address of the individual's current employer(s). If the individual's current employer is the U.S. military service, include branch of service;
- Fingerprints in a manner prescribed by TSA;
- Passport number, city of issuance, date of issuance, and date of expiration (Voluntary but may assist the adjudication process);
- Department of State Consular Report of Birth Abroad (Voluntary but may assist the adjudication process);
- If the individual is not a national or citizen of the United States, the alien registration and/or the number assigned to the applicant on the U.S. Customs and Border Protection Arrival-Departure Record, Form I–94 (Voluntary but may assist the adjudication process);
- Whether the applicant has previously completed a TSA threat assessment, and if so, the date and program for which it was completed (Voluntary but may assist the adjudication process); and
- Federal security clearance, if applicable, and the date the clearance was granted and the name of the agency that processed the clearance (Voluntary but may assist the adjudication process).

Data Retention Requirements

TSA will retain security threat assessment data in accordance with the records retention schedule previously approved for the Transportation Threat Assessment and Credentialing program. Under this record retention schedule, TSA will retain records for one (1) year after an individual's access privilege under the STA is no longer valid. In addition, for those individuals who may originally have appeared to be a match to a watch list, but are subsequently cleared, TSA will retain the records for at least seven years or one year after which access privilege under the STA is no longer valid. For individuals who are an actual match to a watch list or otherwise

determined to pose a threat to transportation or national security, TSA will retain the records for ninety-nine (99) years or seven (7) years after TSA learns the individual is deceased.

TSA is developing a records schedule to cover AOSC contact information, which will be submitted to National Archives and Records Administration (NARA) for review and approval. TSA expects the schedule to allow for the deletion of contact information when it becomes outdated and is no longer accurate. Until a schedule is approved by NARA, TSA will securely maintain all stakeholder POC information. The updated PIA and Final Rule will detail the retention schedule for OOSC contact information.

TSA will propose that auditor reports be retained for at least three years from the date of the last audit inspection. A record retention schedule will be prepared and will be submitted to the National Archives and Records Administration (NARA) for approval as described in Section 3.2. Until the schedule is approved by NARA, TSA will not destroy any audit records.

Data Refresh Rates within Data Framework

Private Charter and Twelve Five Program data is refreshed on a near real-time basis within Data Framework.

16. Secure Flight Confirmed Matches Data

Components Transportation Security Administration (TSA)

Status Approved. The Secure Flight Confirmed Matches data was approved to enter the Data Framework on July 14, 2016.

Description

The Secure Flight program matches identifying information of aviation passengers and certain non-travelers against the consolidated and integrated terrorist watch list maintained by the Federal Government in a consistent and accurate manner, while minimizing false matches and protecting personally identifiable information. Under the Secure Flight program TSA collects limited Secure Flight Passenger Data (SFPD) from certain U.S. aircraft operators and foreign carriers for the purpose of passenger watch list matching against the No Fly and Selectee list components of the Terrorist Screening Database (TSDB) or the full TSDB or other government databases, where warranted by security considerations, such as intelligence or law enforcement databases. This PTA only addresses records for individuals encountered by Secure Flight who are confirmed as matches (SF Confirmed Matches) to the TSDB. SF Confirmed Matches data does not include SFPD for passengers selected for screening based on intelligence rules.

Relevant Compliance Documents

PIA

DHS/TSA/PIA-018(a) Secure Flight Program[42]

Associated SORN(s)

DHS/TSA-011 Transportation Security Intelligence Files[43]

Individuals Covered

Individuals identified in intelligence, counterintelligence, transportation security, or information system security reports and supporting materials, including but not limited to individuals involved in matters of intelligence, law enforcement or transportation security, information systems security, the compromise of classified information, or terrorism.

Data Elements Covered

- Full name;

[42] DHS/TSA/PIA-018(a) Secure Flight Program, *available at* www.dhs.gov/privacy.
[43] DHS/TSA-011 Transportation Security Intelligence Files, 75 FR 18867 (April 13, 2010). Final Rule for Privacy Exemption, 71 FR 44223 (Aug. 4, 2006).

- Date of birth;
- Gender;
- Redress number (if available);
- Known traveler number (if available);
- Encounter; and
- Passport information (if available).

To manage the processing of the SFPD, TSA will require aircraft operators to include in the SFPD the following information: Reservation Control Number; Record Sequence Number; Record Type; Passenger Update Indicator; Traveler Reference Number; and Itinerary information.

Data Retention Requirements

Pursuant to the approved National Archives and Records Administration records retention schedule N1-560-04-12, routine and insignificant case files are destroyed after thirty years; significant case files are retained permanently; watch logs are destroyed after thirty years; watchlists are destroyed 99 years after date of entry or seven years after confirmation of death, whichever is sooner.

Data Refresh Rates within Data Framework

Secure Flight Confirmed Matches data is refreshed on a near real-time basis within Data Framework.