



## Appendix A: Data Framework Data Sets

Appendix A includes details and information on both approved and pending 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 data 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.

Some 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 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.

### **Appendix A: Data Framework Data Sets**

1. Electronic System for Travel Authorization (ESTA) .....	2
2. Alien Flight Student Program (AFSP).....	6
3. Student Exchange Visitor Information System (SEVIS).....	9
4. Advanced Passenger Information System (APIS) .....	13
5. Form I-94.....	18
6. Passenger Name Record (PNR).....	22



## 1. Electronic System for Travel Authorization (ESTA)

<b>Component</b>	U.S. Customs and Border Protection (CBP)
<b>Status</b>	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<sup>1</sup>

#### SORN

DHS/CBP-009 Electronic System for Travel Authorization (ESTA) System of Records<sup>2</sup>

### 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

---

<sup>1</sup> DHS/CBP/PIA-007(d) Electronic System for Travel Authorization (November 3, 2014) *available at* <http://www.dhs.gov/sites/default/files/publications/privacy-pia-update-cbp-esta-11032014.pdf> .

<sup>2</sup> DHS/CBP-009 Electronic System for Travel Authorization (ESTA) System of Records, 79 FR 65414 (November 3, 2014), *available at* <https://www.federalregister.gov/articles/2014/11/04/2014-26100/privacy-act-of-1974-department-of-homeland-security-us-customs-and-border-protection-dhscbp-009> .



categories of records in ESTA include:

- 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.<sup>3</sup>

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 Non-Immigrant Information System

---

<sup>3</sup> [DHS/CBP-003 Credit/Debit Card Data System](http://www.gpo.gov/fdsys/pkg/FR-2011-11-02/html/2011-28406.htm) 76 FR 67755 (November 2, 2011) available at <http://www.gpo.gov/fdsys/pkg/FR-2011-11-02/html/2011-28406.htm>.



(NIIS).<sup>4</sup> This corresponding admission record will be retained in accordance with the NIIS retention schedule, which is 75 years.

### **Data Refresh Rates within Data Framework**

No data refresh agreement with ESTA has been agreed upon to date. Data in Data Framework is current as of early December 2014.

As noted in the Data Framework PIA, to help mitigate the risk due to these manual 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.

---

<sup>4</sup> DHS/CBP-016 Nonimmigrant Information System, 73 FR 77739 (December 19, 2008), *available at* <http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29792.htm>.



## 2. Alien Flight Student Program (AFSP)

<b>Component</b>	Transportation Security Administration (TSA)
<b>Status</b>	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)<sup>5</sup>

#### Associated SORN(s)

DHS/TSA-002 Transportation Security Threat Assessment System SORN<sup>6</sup>

### 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:

---

<sup>5</sup> DHS/TSA/PIA-026 Alien Flight Student Program (AFSP) (July 28, 2014), available at <http://www.dhs.gov/publication/dhs-tsa-pia-026-alien-flight-student-program>.

<sup>6</sup> DHS/TSA-002 Transportation Security Threat Assessment System SORN, 70 FR 33383 (May 19, 2010), available at <http://www.gpo.gov/fdsys/pkg/FR-2010-05-19/html/2010-11919.htm>.



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



## 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)<sup>7</sup>

#### SORN

DHS/ICE-001 Student and Exchange Visitor Information System (SEVIS) System of Records<sup>8</sup>

### Individuals Covered

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

- Prospective, current, and former nonimmigrants<sup>9</sup> 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);

---

<sup>7</sup> DHS/ICE/PIA-001(a) Student Exchange Visitor Information System (SEVIS) (June 23, 2011), available at [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_pia\\_sevis\\_update\\_nctc.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_sevis_update_nctc.pdf).

<sup>8</sup> DHS/ICE-001 Student and Exchange Visitor Information System (SEVIS) System of Records, 75 FR 412 (January 5, 2010), available at <http://www.gpo.gov/fdsys/pkg/FR-2010-01-05/html/E9-31268.htm>.

<sup>9</sup> 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



- 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:

- Names;
- 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:

---

exchange visitor program in the U.S.



- 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**

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



## 4. Advanced Passenger Information System (APIS)

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

**Status** Pending as of February 27, 2015. The approval date for APIS data to enter the Data Framework will be determined following the approval of the Terms and Conditions document with the Office of General Counsel (OGC).

### Description

Advanced 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) Advanced Passenger Information System (APIS)<sup>10</sup>

#### SORN

DHS/CBP-005 Advanced Passenger Information System (APIS) System of Records<sup>11</sup>

### 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

---

<sup>10</sup> DHS/CBP/PIA-001(f) Advanced Passenger Information System (APIS)<sup>10</sup> (June 5, 2013), available at <http://www.dhs.gov/sites/default/files/publications/privacy-pia-apis-update-20130605.pdf>.

<sup>11</sup> DHS/CBP-005 Advanced Passenger Information System (APIS) System of Records, 73 FR 68435 (November 18, 2008), available at <http://www.gpo.gov/fdsys/pkg/FR-2008-11-18/html/E8-27205.htm>.



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

- Complete name;
- Date of birth;
- Gender
- Country of citizenship;
- Passport/alien registration number and country of issuance;
- Passport expiration date;
- Country of residence;
- Status on board the aircraft;
- Travel document type;
- United States destination address (for all private aircraft passengers and crew, and commercial air, rail, bus, and vessel passengers except for U.S. citizens, Lawful Permanent Residents, crew, and those in transit);
- Place of birth and address of permanent residence (commercial flight crew only);
- Pilot certificate number and country of issuance (flight crew only, if applicable);
- 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**

No data refresh rates have been agreed upon with CBP at this time.

As noted in the Data Framework PIA, to help mitigate the risk due to these manual 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** Pending as of February 27, 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 Non-Immigrant Immigration 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<sup>12</sup>

#### Associated SORN(s)

DHS/CBP-005 Advanced Passenger Information System (APIS) System of Records<sup>13</sup>

DHS/CBP-016 Nonimmigrant Information System (NIIS) System of Records<sup>14</sup>

### 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:

---

<sup>12</sup> DHS/CBP/PIA-016 I-94 Automation (February 27, 2013), available at

<https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/pia-cbp-16-I-94-automation-20130227.pdf>.

<sup>13</sup> DHS/CBP-005 Advanced Passenger Information System (APIS) System of Records, 73 FR 68435 (November 18, 2008), available at <http://www.gpo.gov/fdsys/pkg/FR-2008-11-18/html/E8-27205.htm>.

<sup>14</sup> DHS/CBP-016 Nonimmigrant Information System (NIIS) System of Records, 73 FR 77739 (December 19, 2008), available at <http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29792.htm>.



- 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**

No data refresh rates have been agreed upon with CBP at this time.

As noted in the Data Framework PIA, to help mitigate the risk due to these manual 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



**Homeland  
Security**

any product or before the information is used operationally.



## 6. Passenger Name Record (PNR)

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

**Status** Pending as of February 27, 2015. The approval date for PNR data to enter the Data Framework will be determined following the approval of the Terms and Conditions document with the Office of General Counsel (OGC).

### 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;<sup>15</sup>
- *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;*<sup>16</sup>
- A Report on the Use and Transfer of Passenger Name Records between the European Union and the United States.<sup>17</sup>

---

<sup>15</sup> 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](http://www.cbp.gov/sites/default/files/documents/pnr_privacy.pdf).

<sup>16</sup> Available at <http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=9382>.

<sup>17</sup> 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<sup>18</sup>

### Associated SORN(s)

DHS/CBP-006 Automated Targeting System (ATS) System of Records<sup>19</sup>

## 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;

---

<sup>18</sup> DHS/CBP/PIA-006(d) Automated Targeting System (ATS) – TSA/CBP Common Operating Picture Phase II (September 16, 2014) available at

[http://www.dhs.gov/sites/default/files/publications/privacy\\_pia\\_cbp\\_tsacop\\_09162014.pdf](http://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_tsacop_09162014.pdf).

<sup>19</sup> DHS/CBP-006 Automated Targeting System (ATS) System of Records, 77 FR 30297 (May 22, 2012) available at <http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm>.



- All available contact information (including originator of reservation);
- All available payment/billing information (e.g. credit card number);
- Travel itinerary for specific PNR;
- 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
- 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**

No data refresh rates have been agreed upon with CBP at this time.

As noted in the Data Framework PIA, to help mitigate the risk due to these manual 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.