Appendix A Update: Data Management Hub Datasets

Last updated: October 29, 2019

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

Table of Contents

1. Electronic System for Travel Authorization (ESTA)

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

Description

ESTA is a web-based system that DHS/CBP developed in 2008 to determine the eligibility of aliens to travel 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 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:

- Full Name (First, Middle, and Last);
- Other names or aliases, if available;
- Date of birth;
- City of birth;
- Gender;
- Email address;

[1] *See* DHS/CBP/PIA-007 Electronic System for Travel Authorization and subsequent updates, *available at* https://www.dhs.gov/privacy.
[2] DHS/CBP-009 Electronic System for Travel Authorization (ESTA), 84 FR 30746 (June 27, 2019).

- 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 (2) 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 (1) 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. National Archives and Records Administration (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 accordance with 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 Hub

ESTA information will be refreshed in near real time.

Mission Use Case

National Vetting Center (NVC): The Data Management Hub supports the delivery of ESTA vetting support requests to Vetting Support Agencies (VSA) and the consolidation and visualization of relevant matching results from VSAs.

Relevant Documentation: DHS/ALL/PIA-072 National Vetting Center (NVC);[5] NVC Concept of Operations (CONOPS) - Addendum 1.0 (ESTA).

[3] DHS/CBP-003 Credit/Debit Card Data System, 76 FR 67755 (November 2, 2011).
[4] DHS/CBP-016 Nonimmigrant and Immigrant Information System, 80 FR 13398 (March 13, 2015).
[5] *See* DHS/ALL/PIA-072 National Vetting Center (NVC), *available at* https://www.dhs.gov/privacy.

2. Passenger Name Record (PNR)

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

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 United States 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 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;[6]
- *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*;[7] and
- A Report on the Use and Transfer of Passenger Name Records between the European Union and the United States.[8]

Relevant Compliance Documents

DHS/CBP/PIA-006 Automated Targeting System (ATS)[9]

DHS/CBP-006 Automated Targeting System (ATS) System of Records[10]

---

[6] U.S. Customs and Border Protection Passenger Name Record (PNR) Privacy Policy; June 21, 2013, *available at* https://www.cbp.gov/document/forms/passenger-name-record-pnr-privacy-policy.
[7] *Available at* http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=9382.
[8] 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.
[9] *See* DHS/CBP/PIA-006 Automated Targeting System (ATS), *available at* https://www.dhs.gov/privacy.
[10] DHS/CBP-006 Automated Targeting System (ATS) System of Records, 77 FR 30297 (May 22, 2012).

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, 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;
- 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.

Data Retention Requirements

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

- ATS 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 PII 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 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 Hub

PNR data is refreshed on a near real-time basis within the Data Hub.

Mission Use Case

Refer to classified appendix.

3. Advance Passenger Information System (APIS)

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

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

DHS/CBP/PIA-001 Advance Passenger Information System (APIS)[11]

DHS/CBP-005 Advance Passenger Information System (APIS) System of Records[12]

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 overfly the United States.

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;

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

- 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 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. Additionally, for individuals subject to OBIM requirements, a copy of certain APIS data is transferred to the Arrival and Departure Information System (ADIS)[13] for effective and efficient processing of foreign nationals. Different retention periods apply for APIS data contained in those systems.

Data Refresh Rates within Data Hub

APIS data is refreshed on a near real-time basis within the Data Hub.

Mission Use Case

Continuous Evaluation/Travel Record Data Service (CE/TRDS): TRDS is a DHS project, whereby CBP travel records are shared with the Office of the Director of National Intelligence (ODNI) National Counterintelligence and Security Center (NCSC) Continuous Evaluation System (CES). NCSC will provide authorized Executive Branch agencies with TRDS information, via the CES, to continually evaluate the suitability of "covered individuals." NCSC will then share relevant CBP travel information with the covered individual's home agency or authorized Investigative Service Provider to allow that home agency to determine if a security-relevant issue exists.

Relevant Documentation: DHS/ALL/PIA-067 Continuous Evaluation (CE) Travel Record Data Service (TRDS)[14]

[13] *See* DHS/CBP/PIA-024 Arrival and Departure Information System, *available at* https://www.dhs.gov/privacy.
[14] *See* DHS/ALL/PIA-067 Continuous Evaluation (CE) Travel Record Data Service (TRDS), *available at* https://www.dhs.gov/privacy.

4. Border Crossing Information (BCI)

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

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

DHS/CBP-007 Border Crossing Information System of Records[15]

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;
- 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;

[15] DHS/CBP-007 Border Crossing Information System of Records, 81 FR 4040 (December 13, 2016). Please note that multiple PIAs are applicable to this system of records. Please refer to the DHS Privacy website for more information about specific CBP programs that collect BCI.

- 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 Hub

BCI data is refreshed on a near real-time basis within Data Hub.

Mission Use Case

Continuous Evaluation/Travel Record Data Service (CE/TRDS): TRDS is a DHS project, whereby CBP travel records are shared with the Office of the Director of National Intelligence (ODNI) National Counterintelligence and Security Center (NCSC) Continuous Evaluation System (CES). NCSC will provide authorized Executive Branch agencies with TRDS information, via the CES, to continually evaluate the suitability of "covered individuals." NCSC will then share relevant CBP travel information with the covered individual's home agency or authorized Investigative Service Provider to allow that home agency to determine if a security-relevant issue exists.

Relevant Documentation: DHS/ALL/PIA-067 Continuous Evaluation (CE) Travel Record Data Service (TRDS)[16]

[16] *See* DHS/ALL/PIA-067 Continuous Evaluation (CE) Travel Record Data Service (TRDS), *available at* https://www.dhs.gov/privacy.

5. Arrival and Departure Information Systems (ADIS)

Component U.S. Customs and Border Protection

Description

ADIS consolidates data from a variety of systems to create a unique person-centric record with complete travel history. Originally, CBP created ADIS to identify individuals who had overstayed their class of admission ("visa overstays"); however, due to ADIS's unique abilities to conduct biographic matching, data-tagging, and filtering, CBP has broadened ADIS to include all traveler encounters regardless of citizenship.

The system serves as the primary repository used to determine person-centric travel history and immigration status, ADIS data provides a vital role in numerous law enforcement and intelligence missions. In addition, ADIS supports a variety of non- law enforcement use cases that often require U.S. citizen travel history as well as traveler immigration status. CBP is reissuing this PIA to document the expanded uses of ADIS and its maintenance of all CBP travel records, including those of U.S. citizens.

A number of DHS components, in addition to other sources, provide data directly or indirectly to ADIS through system interfaces. ADIS source systems include:

- CBP TECS system,[17] (which includes Person Encounter records created from the Advance Passenger Information System (APIS), traveler crossing records, and the non-immigrant information system database);
- USCIS Computer Linked Application Management System 3 (CLAIMS 3),[18] CLAIMS 4,[19] and Electronic Immigration System (ELIS)[20] (some of this data is retrieved via the Person Centric Query Service[21]);
- U.S. Department of State's (DOS) Consular Consolidated Database (CCD);[22]

[17] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, *available at* https://www.dhs.gov/privacy, and DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008). CBP TECS system also maintains records covered by the DHS/CBP-007 Border Crossing Information, 81 FR 89957 (December 13, 2016) and the DHS/CBP-016 Non-Immigrant Information System, 80 FR 13398 (March 13, 2015). *See also* DHS/CBP/PIA-001 Advance Passenger Information System (APIS), *available at* https://www.dhs.gov/privacy, and DHS/CBP-005 Advance Passenger Information System, 80 FR 13407 (March 13, 2015).

[18] *See* DHS/USCIS/PIA-016 Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems, *available at* https://www.dhs.gov/privacy.

[19] *See* DHS/USCIS/PIA-015 Computer Linked Application Information Management System (CLAIMS 4), *available at* https://www.dhs.gov/privacy.

[20] USCIS recently launched its electronic immigration benefits system, known as USCIS ELIS. The system modernizes the process for filing and adjudicating immigration benefits. For a full explanation, *see* DHS/USCIS/PIA-056 USCIS Electronic Immigration System (USCIS ELIS), *available at* https://www.dhs.gov/privacy, and DHS/USCIS-007 Benefits Information System, 81 FR 72069 (October 19, 2016).

[21] *See* DHS/USCIS/PIA-010 Person Centric Query Service (PCQS), *available at* https://www.dhs.gov/privacy.

[22] *See* Department of State Privacy Impact Assessment for Consular Consolidated Database (CCD) (July 17, 2015),

- Biometric indicators regarding DHS encounters via the Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT);[23] and
- U.S. Immigration and Customs Enforcement (ICE) Student and Exchange Visitor Information System (SEVIS).[24]

This data is used in connection with DHS missions such as national security, law enforcement, immigration, intelligence, and other DHS mission-related functions. Data is also used to provide associated testing, training, management reporting, planning and analysis, or other administrative purposes. Similar data may be collected from multiple sources to verify or supplement existing data and to ensure a high degree of data accuracy.

Specifically, DHS/CBP uses ADIS data to: (1) Identify lawfully admitted non-immigrants who remain in the United States beyond their period of authorized stay (which may have a bearing on an individual's right or authority to remain in the country, ability to receive or renew a U.S. visa, or to receive governmental benefits); (2) assist DHS in supporting inspections at ports of entry (POE) by providing quick retrieval of biographic and biometric indicator data on individuals who may be inadmissible to the United States; (3) facilitate the investigation process of individuals who may have violated their immigration status or may be subjects of interest for law enforcement or intelligence purposes; and (4) and permit non-law enforcement queries of CBP travel data.

Consistent with DHS's information-sharing mission, information stored in ADIS may be shared with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. Information may be shared outside of DHS consistent with applicable exemptions under the Privacy Act, including routine uses that provide for sharing with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies. In addition to a routine use, CBP requires a written Information Sharing and Access Agreement that is agreed upon by all applicable data owners before ADIS data can be shared outside the Data Management Hub.

---

available at https://2009-2017.state.gov/documents/organization/242316.pdf and relevant SORNs: Overseas Citizens Services Records-STATE-05 May 02, 2008, Passport Records – STATE-26 March 24, 2015, Visa Records – STATE-39 October 25, 2012.

[23] Note that IDENT is generally not a source system of DHS information, however, in the case of ADIS, IDENT does provide biometric indicator information to populate an ADIS record. *See* DHS/NPPD/PIA-002 DHS Automated Biometric Identification System (IDENT), *available at* https://www.dhs.gov/privacy, and DHS/NPPD-004 DHS Automated Biometric Identification System, 72 FR 31080 (June 5, 2007). *See* forthcoming Enterprise Biometric Administrative Records SORN, which will provide SORN coverage for the biometric indicators that are generated by IDENT.

[24] *See* DHS/ICE/PIA-001 Student and Exchange Visitor Information System (SEVIS), *available at* https://www.dhs.gov/privacy, and DHS/ICE-001 Student and Exchange Visitor Information System, 75 FR 412 (January 5, 2010).

Relevant Compliance Documents

PIAs:

DHS/CBP/PIA – 024c Arrival and Departure Information System[1]

Associated SORN(s):

DHS/CBP-005 Advance Passenger Information System

DHS/CBP-007 CBP Border Crossing Information

DHS/CBP-011 U.S. Customs and Border Protection TECS

DHS/CBP-016 Non-Immigrant Information System

DHS/CBP-021 Arrival and Departure Information System

DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System

DHS/ICE-001 Student and Exchange Visitor Information System

DOS/Visa Records, STATE-39

Individuals Covered

CBP collects and stores relevant information and demographics specific to travelers entering and/or departing a U.S. port of entry. Categories of individuals consist of aliens who have applied for entry, entered, or departed from the United States at any time. Although this system primarily consists of records pertaining to alien immigrants (including lawful permanent residents) and non-immigrants, some of these individuals may be dual nationals or may change their immigration status and become United States citizens.[25] ADIS's unique filtering capabilities allows for more access controls when sharing data with stakeholders. For example, if there is a stakeholder that only had authority to receive information, either statutorily or through an information sharing agreement with CBP, about non-USCs, ADIS can filter out records about USCs from the data the user receives from the Data Management Hub. Furthermore, for stakeholders who are allowed to access data about USCs but must handle that data differently (vis-à-vis data about non-U.S. persons), ADIS tags the data so the stakeholder can handle it appropriately.

Data Elements Covered

- Biographic data
- Name
- Date of birth

[25] Dual nationals are required by law to travel on their U.S. passport (or alternative documentation as required by 22 CFR part 53) to enter and leave the United States. See INA 215(b) (8 U.S.C. 1185(b)); see also 22 CFR 53.1.

- Nationality
    - Social Security number (SSN), when available; and
    - Other personal descriptive data.
- Biographic Indicator Data
    - Fingerprint identification numbers (FIN)
    - Encounter identification numbers (EID)
    - System-generated identification numbers
- Encounter data
    - Encounter location
    - Arrival and departure dates
    - Flight information
    - Immigration status changes
    - Document types
    - Document numbers
    - Document issuance information
    - Address while in the United States
    - Narrative information entered by immigration enforcement officers
        - Active criminal immigration enforcement investigations
        - Immigration enforcement investigations
        - Immigration status information
        - Details from law enforcement or security incidents or encounters
- Entry or exit data collected by foreign governments in support of their respective entry and exit processes.
- Generally, records collected from foreign governments relate to individuals who have entered or exited the United States at some time, but in some instances, there is no pre-existing ADIS record for the individual.

Data Retention Requirements

The data retention requirement for non-US Citizens is 75 years and 15 years for US Citizens.

Data Refresh Rates within the Data Management Hub

ADIS data is refreshed daily in the Data Management Hub.

Approved Mission Use Cases

Refer to the classified appendix.