Appendix A Update: Data Management Hub Datasets

Last updated: December 20, 2022

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 noncitizens 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 determine 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. If 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

Refer to the classified appendix.

[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).

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;[5]
- *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*;[6] and
- A Report on the Use and Transfer of Passenger Name Records between the European Union and the United States.[7]

Relevant Compliance Documents

DHS/CBP/PIA-006 Automated Targeting System (ATS)[8]

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

---

[5] 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. https://www.cbp.gov/document/forms/passenger-name-record-pnr-privacy-policy.

[6] *Available at* http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=9382.

[7] A Report on the Use and Transfer of Passenger Name Records between the European Union and the United States; July 3, 2013,

[8] DHS/CBP/PIA-006 Automated Targeting System (ATS) – TSA/CBP Commo Operating Picture Phase II, *available at* https://www.dhs.gov/privacy.

[9] See DHS/CBP/PIA-006 Automated Targeting System – January 2017 Addendum Update May 2021, available at www.dhs.gov/privacy; and 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)[10]

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 overfly the United States.

Data Elements Covered

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

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

- Full Name (First, Middle, and Last);
- Date of birth;
- Gender;
- Country of citizenship;
- Passport/A-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 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)[12] 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

Refer to the classified appendix.

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

[12] *See* DHS/CBP/PIA-024 Arrival and Departure Information System, *available at* https://www.dhs.gov/privacy.

time and location of the border crossing.

Relevant Compliance Documents

DHS/CBP-007 Border Crossing Information System of Records[13]

Individuals Covered

Individuals with records stored in BCI include U.S. citizens, lawful permanent residents (LPR), and immigrant and nonimmigrant citizens 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;
- Marks;
- Palm prints;
- Digital fingerprints;
- Photographs;
- Digital iris scans;
- Radio Frequency Identification (RFID) tag number(s) (if land or sea border

[13] 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.

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/A-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 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 regarding 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 undocumented individuals, 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 undocumented individuals 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

Refer to the classified appendix.

5. Non-Immigrant Visa (NIV)

Component U.S. Department of State

Description

NIV issues non-immigrant visas to qualified applicants seeking temporary stay in the United States (U.S.), which are the type of visas most sought by visitors for business, pleasure, or education. NIVs are granted to government officials, treaty traders and treaty investors, exchange visitors, temporary workers, and fiancées of U.S. citizens. NIV supports the Bureau of Consular Affairs mission requirements by automating and streaming posts' capabilities for 1) processing applicant, petition, referral, and diplomatic note data, captured photos, and fingerprints; 2) viewing namecheck, fingerprint IDEWNT and other clearance request results; 3) recording the decision of the adjudicating officer; 4) printing the Machine Readable Visa (MRV); 5) processing Border crossing Cards (BCC); 6) processing boarding foils in lieu of transportation letters, scanning documents, and processing clearances such as Security Advisory Opinions (SAO).

Relevant Compliance Documents

PIAs

Department of State Overseas Consular Support Applications (OCSA)[14]

Department of State Consular Lookout and Support System (CLASS) [15]

Associated SORN(s)

DHS/CBP-016 Nonimmigrant Information System

Visa records STATE-39

Individuals Covered

Individuals with records stored in NIV include U.S. citizens, lawful permanent

[14] Overseas Consular Support Applications PIA, available at www.state.gov/privacy-impact-assessments-privacy-office.
[15] Consular Lookout and Support System PIA, available at www.state.gov/privacy-impact-assessments-privacy-office.

residents (LPR), and immigrant and nonimmigrant individuals.

Data Elements Covered

Refer to the classified appendix.

Data Retention Requirements

NIV data is retained for 11 years from the date of visa creation.

Data Refresh Rates within the Data Management Hub

NIV data is refreshed on a near-real time basis in the Data Hub at a rate of 1mb every minute.

Approved Mission Use Cases

Refer to the classified appendix.

6. Section 1367 Information (1367)

Component U.S. Citizen and Immigration Services

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, undocumented individuals who illegally entered the U.S., undocumented individuals 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

PIAs

DHS/ALL/PIA-046(b) DHS Data Framework Appendix A: Approved Datasets[16]

[16] DHS/ALL PIA-046(b) DHS Data Framework Appendix A, available at www.dhs.gov/sites/default/files/publications/privacy-pia/dhswide/dhsdataframeworkappendixa-february2018.pdf.

Associated SORN(s)

DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records[17]

Individuals Covered

Any information relating to undocumented individuals 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), as victims of a severe form of human trafficking who generally are cooperating with law enforcement authorities, or as undocumented individuals 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 several immigration benefits, not just the Form I-360 VAWA self-petition. If an undocumented individual 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:

- 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 serve form of trafficking in persons under INA 101(a)(15)(T); and
- I-918 U Nonimmigrant Status – victim of qualifying criminal activity under

[17] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017).

INA 101(a)(15)(U).

Data Elements Covered

USCIS collects and stores the following records as Section 1367 information:

- A-Number;
- Last name;
- First name;
- Middle name;
- Date of birth;
- Gender;
- COA;
- Entry date;
- Country of birth;
- Country of citizenship;
- Port of entry;
- File open date;
- I94 identification number;
- Passport ID number;
- FBI ID number;
- Fingerprint ID number.

Data Retention Requirements

The record is removed after the name stops appearing on the VAWA list.

Data Refresh Rates within the Data Management Hub

Section 1367 data is refreshed daily in the Data Hub.

Approved Mission Use Case

Refer to the classified appendix.

Source List:

DHS SCG I&A-001.4, dated October 2016

NSA/CSSM I-52, dated 10 Jan 2018

DHS/ALL/PIA-046(b) DHS Data Framework Appendix A, dated 14 Feb 2018

7. Biometric Identification Transnational Migration Alert Program (BITMAP) Section 1367 Information (1367)

Description

BITMAP is an HSI-led program supported by the US Border Patrol that allows foreign law enforcement (LE) counterparts, Transnational Criminal Investigative Units (TCIUs), and USBP vetted units to collect and share biometric and biographic data on suspect individuals. BITMAP is currently in use with over 50 law enforcement agencies in 18 countries.

Individuals Covered

PIAs

DHS/OBIM/PIA-001 Automated Biometric Identification System and Appendices[18]

Associated SORN(s)

DHS/ALL-041 External Biometric Records (EBR) System of Records[19]

DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR) System of Records[20]

Individuals Covered

Refer to the classified appendix.

Data Elements Covered

The U.S. and partner nations collect and store the following records in the DH:

- Activity Encounter Identification Number (Activity EID);
- Activity Type;
- A-Registration Number (A#);
- Date of Birth (YY-MM-DD);
- Candidate Encounter Identification Number (EID);

[18] See DHS/OBIM/PIA-001 Automated Biometric Identification System (IDENT) Appendices – November 2019, available at www.dhs.gov/privacy-impact-assessments.
[19] DHS/ALL-041 External Biometric Records (EBR) System of Records, 83 FR 17829 (April 24, 2018).
[20] DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR) System of Records, 85 FR 14955 (March 16, 2020).

- Candidate Organization Name, Unit, Subunit (OUS);
- Date of Encounter Record Request;
- Derogatory Information (DI);
- Department of Defense (DoD) Biometric Identity (BID);
- DoD Transaction Control Number (TCN);
- Encounter Date/Date Fingerprinted;
- FBI Num;
- First name;
- Gender;
- Last Name;
- Location Fingerprinted;
- Match Candidate Fingerprint Identification Number (FIN);
- Nationality;
- National Unique Identification Number (NUIN);
- OUS;
- Passport Number;
- Reason Fingerprinted;
- Shareable Candidate;
- Shared DI;
- Special Protected Class (SPC);
- Transaction EID;
- Unique Candidate Identifier (UCI);
- Watchlist Candidate.

Data Retention Requirements

Refer to the classified appendix.

Data Refresh Rates within Data Management Hub

Refer to the classified appendix.

Approved Mission Use Cases

Refer to the classified appendix.

Source List:

Refer to the classified appendix.

8. Secure Real Time Platform (SRTP)

Description

SRTP is a capability developed and managed by the United States Department of Homeland Security with immigration and border authorities from Australia, Canada, New Zealand, and the United Kingdom that allows foreign governments to reciprocally conduct large scale biometric matching and information sharing, in order to better prevent fraud and criminality, while facilizing international travel. Other participating countries include Greece, Mexico, Bulgaria, Croatia, and Italy.

Relevant Compliance Documents

PIAs

DHS/OBIM/PIA-001 Automated Biometric Identification System and Appendices[21]

Associated SORN(s)

DHS/ALL-041 External Biometric Records (EBR) System of Records[22]

DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR) System of Records[23]

Individuals Covered

Refer to the classified appendix.

Data Elements Covered

The U.S. and partner nations collect and store the following records in the DH:

- Activity Encounter Identification Number (Activity EID);
- Activity Type;

[21] See DHS/OBIM/PIA-001 Automated Biometric Identification System (IDENT) Appendices – November 2019, available at www.dhs.gov/privacy-impact-assessments.
[22] DHS/ALL-041 External Biometric Records (EBR) System of Records, 83 FR 17829 (April 24, 2018).
[23] DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR) System of Records, 85 FR 14955 (March 16, 2020).

- A-Number (A#);
- Date of Birth (YY-MM-DD);
- Candidate Encounter Identification Number (EID):
- Candidate Organization Name, United, Subunit (OUS);
- Date of Encounter Record Request;
- Derogatory Information (DI);
- Department of Defense (DoD) Biometric Identity (BID);
- DoD Transaction Control Number (TCN);
- Encounter Date/Date Fingerprinted;
- FBI Num;
- First name;
- Gender;
- Last Name;
- Location Fingerprinted;
- Match Candidate Fingerprint Identification Number (FIN);
- Nationality;
- National Unique dentification Number (NUIN);
- OUS;
- Passport Number;
- Reason Fingerprinted;
- Sharable Candidate;
- Shared DI;
- Special Protected Class (SPC);
- Transaction EID;
- Unique Candidate Identifier (UCI); and
- Watchlist Candidate.

Data Retention Requirements

Refer to the classified appendix.

Data Refresh Rates within Data Management Hub

Refer to the classified appendix.

Approved Mission Use Cases

Refer to the classified appendix.

Source List:

Refer to the classified appendix.

9. Biometric Data Sharing Program (BDSP) Section 1367 Information (1367)

Description

BDSP is an automated biometrics solution developed for the Government of Mexico's National Institute of Migration that assists in the identification of Third Country Nationals traveling through Mexico. BDSP supports the exchange of biometric information between Mexico and the United States to improve regional security along the Southwest border, better identify transnational criminal threats, and bolster U.S. national security through the identification of special interest aliens (SIA).

Relevant Compliance Documents

PIAs

DHS/OBIM/PIA-001 Automated Biometric Identification System and Appendices[24]

Associated SORN(s)

DHS/ALL-041 External Biometric Records (EBR) System of Records[25]

DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR) System of Records[26]

Individuals Covered

Refer to the classified appendix.

[24] See DHS/OBIM/PIA-001 Automated Biometric Identification System (IDENT) Appendices – November 2019, available at www.dhs.gov/privacy-impact-assessments.
[25] DHS/ALL-041 External Biometric Records (EBR) System of Records, 83 FR 17829 (April 24, 2018).
[26] DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR) System of Records, 85 FR 14955 (March 16, 2020).

Data Elements Covered

The U.S. and partner nations collect and store the following records in the DH:

- Activity Encounter Identification Number (Activity EID);
- Activity Type;
- A-Number (A#);
- Date of Birth (YY-MM-DD);
- Candidate Encounter Identification Number (EID);
- Candidate Organization Name, Unit, Subunit (OUS);
- Date of Encounter Record Request;
- Derogatory Information (DI);
- Department of Defense (DoD) Biometric Identity (BID);
- DoD Transaction Control Number (TCN);
- Encounter Date/Date Fingerprinted;
- FBI Num;
- First name;
- Gender;
- Last Name;
- Location Fingerprinted;
- Match Candidate Fingerprint Identification Number (FIN);
- Nationality;
- National Unique Identification Number (NUIN):
- OUS;
- Passport Number;
- Reason Fingerprinted;
- Shareable Candidate;
- Shared DI;
- Special Protected Class (SPC);

- Transaction EID;
- Unique Candidate Identifier (UCI); and
- Watchlist Candidate.

Data Retention Requirements

Refer to the classified appendix.

Data Refresh Rates within Data Management Hub

Refer to the classified appendix.

Approved Mission Use Cases

Refer to the classified appendix.

Source List:

Refer to the classified appendix.

10. 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.

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

- CBP TECS system,[27] (which includes Person Encounter records created from the

[27] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, *available at*

Advance Passenger Information System (APIS), traveler crossing records, and the non- immigrant information system database);

- USCIS Computer Linked Application Management System 3 (CLAIMS 3), [28] CLAIMS 4,[29] and Electronic Immigration System (ELIS)[30] (some of this data is retrieved via the Person Centric Query Service[31]).
- U.S. Department of State's (DOS) Consular Consolidated Database (CCD);[32]
- Biometric indicators regarding DHS encounters via the Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT);[33] and
- U.S. Immigration and Customs Enforcement (ICE) Student and Exchange Visitor Information System (SEVIS).[34]

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-

---

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).

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

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

[30] 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).

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

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

[33] 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.

[34] *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, DHS/ICE-001 Student and Exchange Visitor Information System, 86 FR 69663 (December 8, 2021).

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.

Relevant Compliance Documents

PIAs:

DHS/CBP/PIA-024c Arrival and Departure Information System
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 undocumented individuals who have applied for entry, entered, or departed from the United States at any time. Although this system primarily consists of records pertaining to

undocumented individuals (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.[35] 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 can 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
- 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

[35] 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.

- 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.

11. NVC Enduring Welcome

Component **National Vetting Center**

Description

Enduring Welcome (EW), formerly Operation Allies Welcome (OAW) describes the coordinated efforts across the federal government to support vulnerable individuals in Afghanistan, including those who worked alongside U.S. personnel for the past two decades, as they safely resettle in the United States. The National Vetting Governance Board (NVGB) authorized support to the EW parole program through the NVC process and technology for an initial period of 90 days, to meet the timelines of EW and to ensure EW parolees are resettled

as soon as possible.

Relevant Compliance Documents

PIAs:

DHS/ALL/PIA-072 National Vetting Center (NVC)[36]

Associated SORN(s):

DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records;[37]

DHS/USCIS-007 Benefits Information System;[38]

DHS/USCIS-010 Asylum Information and Pre-Screening System of Records;[39]

DHS/USCIS-017 Refugee Case Processing and Security Screening Information System of Records;[40]

DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records;[41]

DHS/CBP-006 Automated Targeting System;[42] and

DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER).[43]

Individuals Covered

EW parolees between the ages of 14 and 79 years old.

Data Elements Covered

The following personally identifiable information (PII) may be included in a Vetting Support Request:

[36] See DHS/ALL/PIA-072 Privacy Impact Assessment for the National Vetting Center (NVC), available at www.dhs.gov/privacy-impact-assessments.
[37] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017).
[38] DHS/USCIS-007 Benefits Information System, 84 FR 54622 (October 10, 2019).
[39] DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 774781 (November 30, 2015).
[40] DHS/USCIS-017 Refugee Case Processing and Security Screening System of Records, 81 FR 72075 (October 19, 2016).
[41] DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, 83 FR 36950 (July 31, 2018).
[42] DHS/CBP-006 Automated Targeting System (ATS), 77 FR 30297 (May 22, 2012).
[43] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (October 19, 2016).

- A-Number
- Fingerprint Identification Number
- Full Name
- Aliases
- Date of Birth
- Place of Birth
- Country of Citizenship
- Country of Origin
- Gender
- Travel Document Information
- Form I-94 Number
- Physical Address
- Mailing Address
- Phone Number
- Email Address

Data Retention Requirements

The NVC will retain EW Vetting Records, which include the Vetting Support Request, Vetting Support Response, Analyst Notes (if applicable), Analyst recommendation, and Adjudication for a period of two years, which parallels the two-year parole period granted to many individuals under EW.

EW Vetting Support Agencies are authorized to retain the EW Vetting Records for 90 days while operating under the NVC processes and technology, pursuant to the National Vetting Governance Board's authorized support to the EW parole program.

EW Vetting Support Agencies are separately authorized to temporarily maintain EW Vetting Records outside NVC process and technology for up to one year from the time of receipt for the limited purpose of providing recurrent vetting support, unless identified as retainable by an EW Vetting Support Agency in accordance with its Attorney General Guidelines, or identified by a law enforcement agency or administrative agency as retainable in a Privacy Act compliant system. In such cases, a record may be retained for a longer period in accordance with the applicable records retention schedules and individual authorities to retain the information.

Data Refresh Rates within Data Management Hub

The DMH data refreshes daily.

Approved Mission Use Cases

Refer to the classified appendix.

Relevant Documentation:

DHS/ALL/PIA-072 National Vetting Center (NVC) (September 2022), available at https://www.dhs.gov/publication/dhsallpia-072-national-vetting-center-nvc.

12. Advanced Travel Information System (ATIS)

Component **National Vetting Center**

Description

The Advance Travel Information System (ATIS) is the host system for the data consumed in the Advance Travel Authorization (ATA) process. The ATA process is the process through which the National Vetting Center is facilitating vetting by the U.S. Department of Homeland Security (DHS) of noncitizens from certain countries who are requesting authorization to travel to the United States to seek a discretionary grant of parole. This Addendum outlines how eligible individuals may request such travel authorization, and the process by which the appropriate screening and vetting is conducted so that adjudicators can make fully informed decisions.

The screening and vetting process for individuals in the ATA process is as follows. First, a supporting individual or entity based in the United States (U.S. supporter) will submit a signed- I-134, *Declaration of Financial Support*, via the *myUSCIS* portal.[44] This declaration will include biographic information on the U.S. supporter and the foreign national(s) and eligible family members whom they intend to support (beneficiary). U.S. Citizenship and Immigration Services (USCIS) will vet the U.S. supporter, conduct the appropriate financial verification and background checks. In addition, USCIS will confirm the beneficiary's biographic information, and confirm the beneficiary's attestation of vaccination against measles, polio, and COVID-19. Following approval of the I-134, USCIS will assign each traveler an A-Number if they do not already have an assigned A-Number and will notify the traveler electronically with an invitation to create a *myUSCIS* account. *myUSCIS* is a USCIS-owned digital environment where individuals create a secure account to use various digital services and access pending case information. Once in *myUSCIS*, the beneficiary or

[44] The *myUSCIS* portal may be found at https://my.uscis.gov.

beneficiaries will be required to review and verify their biographic information as provided on the I-134 is accurate and to attest to completion of all additional requirements.

Once the *myUSCIS* enrollment process is complete, a copy of beneficiaries' biographic data is sent to the Automated Targeting System (ATS) maintained by U.S. Customs and Border Protection (CBP), where it is vetted against select DHS and other federal agency security and law enforcement databases for national security, border security, public health, and safety concerns. CBP conducts this vetting to determine whether the beneficiary poses a security risk to the United States and whether they are eligible to obtain advance authorization to travel to the United States to seek a discretionary grant of parole. This process will include classified vetting facilitated by the process and technology of the National Vetting Center (NVC).

Once the traveler has confirmed their biographic information, *myUSCIS* will inform the traveler to complete their request for advance authorization to travel by downloading and using the CBP One™ mobile application to submit biographic and biometric data. This process is explained in detail in the CBP One Privacy Impact Assessment (PIA).[45]

Relevant Compliance Documents

PIAs:

DHS/ALL/PIA-072 National Vetting Center (NVC)[46]

DHS/CBP/PIA-073 Advance Travel Authorization

DHS/CBP/PIA-068 CBP One Mobile Application

Associated SORN(s):

DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records;[47]

DHS/USCIS-007 Benefits Information System;[48]

DHS/USCIS-010 Asylum Information and Pre-Screening System of Records;[49]

DHS/USCIS-017 Refugee Case Processing and Security Screening Information

[45] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE CBP ONE ™, DHS/ALL/PIA-068 (February 19, 2021, and subsequent updates to appendices) *available at* https://www.dhs.gov/privacy-impact-assessments.
[46] DHS/ALL/PIA-072 Privacy Impact Assessment for the National Vetting Center (NVC) December 11, 2018, available at www.dhs.gov/privacy-impact-assessments
[47] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017)
[48] DHS/USCIS-007 Benefits Information System, 84 FR 54622 (Oct 10, 2019)

[49] DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 774781 (November 30, 2015).

System of Records;[50]

DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records;[51]

DHS/CBP-006 Automated Targeting System;[52] and

DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER)[53]

Individuals Covered

Please visit https://www.dhs.gov/publication/dhscbppia-073-advance-travel-authorization-ata for the current list of countries in which citizens and their qualified family members from those countries are eligible to participate in the ATA process. The list of ATA countries is included in Appendix A to DHS/CBP/PIA-073 Advance Travel Authorization.

Data Elements Covered

The following personally identifiable information (PII) may be included in a Vetting Support Request:

- A-Number
- Fingerprint Identification Number (FIN)
- Full Name (First, Last, Middle)
- Aliases
- Date of Birth
- Place of Birth
- Country of Citizenship/Nationality
- Country of Origin
- Sex/Gender
- Travel Document Information (e.g., passport number, passport expiration)

[50] DHS/USCIS-017 Refugee Case Processing and Security Screening System of Records, 81 FR 72075 (October 19, 2016).
[51] DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, 83 FR 36950 (July 31, 2018).
[52] DHS/CBP-006 Automated Targeting System (ATS), 77 FR 30297 (May 22, 2012).
[53] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (October 19, 2016).

- Form I-94 Number
- Physical Address
- Mailing Address
- Phone Number
- Email Address

Data Retention Requirements

The DMH will retain ATA Vetting Records, which include the Vetting Support Request, Vetting Support Response, Analyst Notes (if applicable), Analyst recommendation, and Adjudication for a period of two years, which parallels the two-year parole period granted to many individuals under Operation Enduring Welcome.

ATA Vetting Support Agencies are authorized to retain the ATA Vetting Records for 90 days while operating under the NVC processes and technology, pursuant to the National Vetting Governance Board's authorized support to the ATA parole program.

ATA Vetting Support Agencies are separately authorized to temporarily maintain ATA Vetting Records outside NVC process and technology for up to two years from the time of receipt for the limited purpose of providing recurrent vetting support, unless identified as retainable by an ATA Vetting Support Agency in accordance with its Attorney General Guidelines, or identified by a law enforcement agency or administrative agency as retainable in a Privacy Act compliant system. In such cases, a record may be retained for a longer period in accordance with the applicable records retention schedules and individual authorities to retain the information.

Data Refresh Rates within Data Management Hub

The DMH data refreshes in near real time.

Approved Mission Use Cases

ATA Parole Eligibility and Termination Support: I&A will store the data in the DMH on behalf of CBP and NVC. CBP will use the information to determine the eligibility of the beneficiary to travel to the United States, including whether the individual poses a law enforcement or security risk. With the addition of the vetting support provided through the NVC process, CBP will be better equipped to identify travelers of interest and distinguish them from those who do not pose a higher risk, thereby improving its security capabilities while also more efficiently facilitating the travel of those who do not pose a security risk.

CBP will continue to vet beneficiary information against selected security and law enforcement databases at DHS outside of the NVC process while also employing the NVC process and technology to compare against Vetting Support Agencies' holdings as well.

The sharing and use of information made available to CBP by Vetting Support Agencies is governed by the documentation approved by the National Vetting Governance Board that authorizes this vetting support, which is attached as an addendum to the classified NVC CONOP, along with the Vetting Support Agencies' guidelines and policies applicable to the sharing of intelligence, law enforcement, or other information. Vetting Support Agencies that are elements of the Intelligence Community must determine that sharing intelligence with CBP is permitted under their Attorney General Guidelines for the protection of U.S. person information, which are mandated by Executive Order 12333 and other applicable procedures, before they may provide it to CBP through the NVC process and technology.

Relevant Documentation:

DHS/ALL/PIA-072 National Vetting Center (NVC) (September 2022), available at https://www.dhs.gov/publication/dhsallpia-072-national-vetting-center-nvc.