Privacy Impact Assessment
for

Arrival and Departure Information System (ADIS)

DHS/CBP/PIA-024(c)

January 3, 2020

Contact Point
Michael J. Gorman
Enterprise Reporting & Data Systems
Office of Field Operations
U.S. Customs and Border Protection
(202) 344-3636

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) Arrival and Departure Information System (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 is broadening its use of ADIS for all traveler encounters regardless of citizenship. CBP is republishing this Privacy Impact Assessment (PIA) to provide notice, and assess the privacy risks, of expanding ADIS beyond its original visa overstay mission. As the primary CBP system 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.

Overview

The former Immigration and Naturalization Service (INS) originally developed the ADIS in 2002 to meet the requirements of Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, which mandated the development of an automated entry and exit control system and the matching of foreign nationals' arrival and departure records.[1] DHS, the successor to INS, operates ADIS to meet this mandate.

ADIS's original purpose was to match arrival and departure[2] records so DHS can determine the number of individuals who arrive, but for whom no record of departure exists ("in-country overstays"), as well as those for whom there are records of departure but who had stayed in the United States beyond their "Admit Until Date (AUD)" ("out-of-country overstays"). DHS has faced a challenge in identifying overstays and generating full traveler history due to the lack of nationwide departure control infrastructure. In general, transportation hubs and border infrastructure in the United States were not constructed with exit processing in mind. For example, airports in the United States do not have areas designated exclusively for travelers leaving the United States. Instead, travelers' departures are recorded biographically using outbound passenger

[1] Pub. L. 104-208, 110 Stat. 3009-546.
[2] The collection and transmission of electronic departure Advanced Passenger Information System (APIS) data, of all persons, to immigration officers became mandatory under the "Making appropriations for the Departments of Commerce, Justice, and State, the Judiciary, and related agencies for the fiscal year ending September 30, 2002, and for other purposes" (P.L. 107-77, Sec 115(b), Departure Manifest, Form and Content. This Act modified Section 231 of the Immigration and Nationality Act).

manifests provided by commercial carriers. Carriers also are required to validate the manifest against the travel document presented by the traveler before he or she is permitted to board his or her aircraft or sea vessel. While DHS continues to address this challenge through the development of biometric-based exit programs,[3] DHS uses the ADIS system to conduct biographic matching to determine a traveler's full travel history and arrival and departure information.

Until 2013, the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program[4] within the DHS National Protection and Programs Directorate (NPPD)[5] managed ADIS. The 2013 Consolidated and Further Continuing Appropriations Act[6] transferred responsibility for the entry/exit mission from US-VISIT to CBP. This transfer created the Entry/Exit Transformation Office within CBP's Office of Field Operations. With the 2014 Consolidated Appropriations Act,[7] Congress directed DHS to move ADIS to CBP to align the entry/exit database with the entry/exit mission office.

Identifying Overstays

Since 2013, ADIS has enabled DHS to better track overstays[8] by compiling information from a variety of federal systems to create a complete travel profile of an individual using his or her travel history. In order to calculate a complete travel history for an individual and determine whether an individual has violated the terms of admission into the United States, ADIS collects arrival and departure information, class of admission (COA) information, and immigrant benefit information from external sources to determine whether an individual is an overstay.

Determining lawful status requires more than solely matching entry and exit data. For example, a person may receive a six-month admission from CBP upon entry, and then he or she may subsequently apply for and receive from U.S. Citizenship and Immigration Services (USCIS)

[3] DHS/CBP/PIA-056 Traveler Verification Service (November 2018) describes the CBP biometric entry/exit solution to record arrivals and departures to and from the United States. Following several years of testing and pilots, CBP has successfully operationalized and deployed facial recognition technology, now known as the Traveler Verification Service (TVS), to support comprehensive biometric entry and exit procedures in the air, land, and sea environments. *Available at* https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service-0.
[4] The Office of Biometric Identity Management (OBIM) was created in March 2013, replacing the US-VISIT Program. OBIM supports DHS's responsibility to protect the nation by providing biometric identification services that help federal, state, and local government decision makers accurately identify the people they encounter and determine whether those people pose a risk to the United States. OBIM supplies the technology for collecting and storing biometric data, provides analysis, updates its watchlist, and ensures the integrity of the data.
[5] In 2018, NPPD became the Cybersecurity and Infrastructure Security Agency (CISA).
[6] Pub. L. 113–6.
[7] Pub. L. 113-32.
[8] An overstay is a nonimmigrant who was lawfully admitted to the United States for an authorized period but remained in the United States beyond his or her authorized period of admission. The authorized admission period can be a fixed period; or for the duration of a certain activity, such as the period during which a student is pursuing a full course of study or any authorized technical/practical training.

an extension of up to six months. Identifying extensions, changes, or adjustments of status are necessary steps to determine whether a person has overstayed their authorized period of admission.

Due to the decentralized nature of admission and immigration information, as well as the lack of a nationwide departure control system, CBP designed ADIS to collect different data points from different data sets to create a "complete travel history" of an individual traveler. CBP and other DHS components manage a variety of systems that house this information; whereas normally DHS users would need to manually research and combine these elements to determine an individual's status, ADIS automates this work by bringing together the data from the variety of source systems.

ADIS aggregates the following data from various systems to create a person-centric view of a traveler to determine full travel history:

- Date the individual entered the United States;
- Class of admission;
- Updates or changes to the individual's immigration status; and
- When available, the date the individual departed the United States.

Form I-94 and Form I-94W

Form I-94 and Form I-94W are the DHS arrival/departure records issued to aliens upon admittance to the United States, and in some cases may be updated or issued when an individual is adjusting or extending status while in the United States, among other scenarios. A CBP officer used to attach the paper Form I-94 or Form I-94W to the non-immigrant visitor's passport upon U.S. entry. The visitor was required to exit the United States on or before the departure date stamped on the I-94 or I-94W.

Given its ability to automatically match arrivals and departure records together, ADIS was also designed to replace the Form I-94, *Arrival and Departure Record*[9] or *Form I-94W Nonimmigrant Visa Waiver Arrival/Departure Record*.[10] Beginning in 2012, ADIS started providing the I-94 system with departures (matched to the corresponding arrival on the I-94) in order to automate Form I-94, shifting CBP away from relying on paper forms for many travelers. CBP uses ADIS to automate the Form I-94 to increase efficiency, reduce operating costs, and streamline the admissions process. CBP has automated Form I-94 at air and sea ports of entry. The paper form will no longer be provided to a traveler upon arrival, except in limited circumstances.[11] Those who need to prove their legal-visitor status—to employers, schools/universities, or

[9] *Available at* https://www.cbp.gov/document/forms/form-i-94-arrivaldeparture-record.
[10] *Available at* https://www.cbp.gov/document/forms/form-i-94w-visa-waiver-arrivaldeparture-record.
[11] CBP now gathers travelers' arrival/departure information automatically from their electronic travel records. Because advance information is only transmitted for air and sea travelers, CBP will still issue a paper form I-94 at land border ports of entry.

government agencies—can access their CBP arrival/departure record information online from www.cbp.gov/I94. The I-94 system was scheduled to be integrated into the ADIS database in November 2020, as the I-94 system has become duplicative to ADIS data.[12]

Traveler Compliance and Law Enforcement Support

ADIS supports the entry/exit mission by consolidating entry, exit, and admission status information from several DHS components, United States Department of State (DOS), and the Canada Border Services Agency (CBSA) in near-real time. CBP plans to add data from other governments, such as that of Mexico, in the future to provide a more complete picture of the entry/exit environment. This information supports DHS mission-related functions and assists other federal agencies by:

- Facilitating the identification and investigation of individuals who may have violated their terms of admission;
- Assisting in the determination of immigration benefits eligibility (including U.S. visas);
- Assisting in the investigation of individuals who may be subjects of interest for national security, law enforcement, immigration, border management, and intelligence purposes;
- Assisting DHS and other Federal Government agencies in conducting background checks on foreign nationals entering DHS or other Federal Government facilities;
- Assisting Federal Government agencies with the adjudication of Federal Government benefits;
- Assisting DHS and other federal programs that require international travel data to generate statistical reports on international visitation and overstay rates; and
- Providing associated testing, training, management reporting, and planning and analysis tools for administrative purposes.

ADIS Source Systems

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

[12] For additional information about the I-94 automation process and the I-94 public-facing website and search, please see DHS/CBP/PIA-016 I-94 Website Application, *available at* https://www.dhs.gov/publication/us-customs-and-border-protection-form-i-94-automation.

- CBP TECS system,[13] (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),[14] CLAIMS 4,[15] and Electronic Immigration System (ELIS)[16] (some of this data is retrieved via the Person Centric Query Service[17]);
- U.S. Department of State's (DOS) Consular Consolidated Database (CCD);[18]
- Biometric indicators regarding DHS encounters via the Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT);[19] and
- U.S. Immigration and Customs Enforcement (ICE) Student and Exchange Visitor Information System (SEVIS).[20]

[13] *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).

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

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

[16] 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).

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

[18] *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.

[19] 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.

[20] *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).

ADIS Information Sharing

CBP provides access to ADIS information to many DHS components, including USCIS, ICE, OBIM, the Transportation Security Administration (TSA), the DHS Office of the Chief Security Officer (OCSO), and other offices as outlined in Appendix A. Consistent with DHS policy, CBP shares information stored in ADIS with other DHS components for entry/exit tracking purposes and mission support.

CBP also allows agencies external to DHS to access ADIS information in support of immigration management, counterterrorism, and other missions consistent with the DHS mission, or as required by law. These external partners include DOS Consular Affairs, the FBI, and the Intelligence Community, among others.[21] Appendix B contains a complete list of external agencies with whom CBP shares ADIS information.

CBP requires a written Information Sharing and Access Agreement, such as a memorandum of understanding (MOU), before providing non-DHS users with a system user account or access to ADIS data extracts. All non-DHS users are employees or contractors supporting Federal Government agencies. DHS components are not required to enter into MOUs with CBP. Further discussion of ADIS uses are covered in Appendix A (DHS users) and Appendix B (external users) of this PIA. These agreements provide the conditions of sharing or disclosure, including governing the protection and use of the information.

ADIS users can access ADIS data through four methods: the ADIS Web and ADIS-R (Reporting) applications, ADIS Web services and other system-to-system interfaces, or data extracts.

- **ADIS Web & ADIS-R** applications allow ADIS users to directly access ADIS data via network authentication. Users are issued a unique user ID and a user password to maintain for ADIS access.
- **ADIS Web Services** is a messaging service that allows users of another authorized system with direct connectivity to ADIS (e.g., the Consular Consolidated Database, or CCD) to send requests and view information from ADIS through that authorized system.
- **System-to-system interfaces** facilitate the ingestion of ADIS data into select IT systems.
- A **data extract** is a copy of a subset of the ADIS database that is encrypted and transmitted to authorized users.

[21] The U.S. Intelligence Community is defined in the National Security Act of 1947, as amended [50 U.S.C. § 401a].

Expansion to Include U.S. Citizen Information

ADIS serves as the traveler compliance system within CBP, which means that it contains person-centric travel records without any information that is law enforcement sensitive. Access to and use of ADIS is preferable for users who do not need access to law enforcement sensitive information but who are still conducting inquiries into traveler records or other non-law enforcement uses. In these situations, ADIS's combination of person-centric and event-based records have proven valuable beyond solely identifying overstays. ADIS removed the manual effort required to review all non-law enforcement travel and immigration events linked to one person across various DHS systems. This functionality led to the system's expanded use by:

- CBP officers and agents, for whom a query of ADIS was quicker and easier than multiple queries of TECS and the other source systems;
- External partners requesting CBP travel data, who needed person-centric records that could be filtered by population type;
- CBP and DHS leadership, who increasingly used ADIS data for reporting purposes due to its ease and reliability; and
- CBP Headquarters and DHS to identify first time travelers having made initial entry into the United States, which supports numerous missions across the Government (e.g., first time Visa Waiver Program travelers in support of calculating biometric volumes, first time refugees for improved processing at ports of entry).

Because ADIS was historically used only in support of the overstay vetting mission, all known U.S. citizen data (identified by travel document information) was filtered out of the system upon ingestion from TECS. As a result, ADIS could only be used for queries related to non-U.S. citizens. To further facilitate the new use cases for ADIS, CBP will now allow ADIS to use the full database of travel records from TECS. CBP expects the maintenance of U.S. citizen travel records in ADIS to lead to the following benefits:

- Improved usability and accuracy of CBP travel records. Person-centric travel record queries allow users to quickly and easily view an individual's entire travel history, with less manual effort and reduced risk of user error due to misidentification or improper correlation. The inclusion of U.S. citizen information means that users will no longer have to check ADIS information against other systems to determine whether a person is actually a citizen.
- Better filtering and access control. Existing methods of sharing travel records require CBP system owners to share records from, or grant access to, databases that also contain sensitive law enforcement information. These systems have limited capabilities of restricting access to certain types of records. By contrast, sharing travel records from

ADIS eliminates the risk of improper sharing of law enforcement information, and its data tagging capabilities help ensure adequate protection of information as required by law, such as information protected from disclosure under 8 U.S.C. § 1367.

- Enhanced accuracy of overstay identifications. Including U.S. citizen data in ADIS will allow CBP to better identify dual nationals[22] who travel on a foreign passport and, without evidence of U.S. citizenship, may have otherwise appeared to be overstays, which may have resulted in the inaccurate creation of overstay notices.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The principal legal authorities that support DHS's maintenance, use, and sharing of ADIS as an entry and exit program necessary to identify foreign nationals who remain in the United States beyond their authorized period of admission include:

- Title 6 of the United States Code, Domestic Security,[23] including:
  - Functions of the Secretary of Homeland Security; and
  - Responsibilities of the Secretary of Homeland Security.
- Title 8 of the United States Code, Aliens and Nationality,[24] including:
  - Powers and duties of the Secretary of Homeland Security;
  - Travel control of citizens and aliens;
  - Inspection by immigration officers; expedited removal of inadmissible arriving aliens; referral for hearing;
  - Issuance of visas;
  - Integrated entry and exit data system;
  - Biometric entry and exit data system;
  - Program to collect information relating to nonimmigrant foreign students and other exchange program participants;

[22] 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.
[23] 6 U.S.C. §§ 112(b) and 202.
[24] 8 U.S.C. §§ 1103, 1185, 1201, 1225, 1365a, 1365b, 1372, 1373, 1379, 1721, 1722, and 1731.

- Communication between government agencies and the Immigration and Nationality Service;
- Technology standard to confirm identity;
- Interoperable means to share information;
- Interim measures for access to and coordination of law enforcement and other information;
- Interoperable law enforcement and intelligence data system with name-matching capacity and training; and
- Implementation of an integrated entry and exit data system.

- Title 42 of the United States Code, The Public Health and Welfare (Reporting information to the Social Security Administration);[25]
- Homeland Security Presidential Directive 6, Integration and Use of Screening Information (September 16, 2003);
- Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection (December 17, 2003);
- Homeland Security Presidential Directive 11, Comprehensive Terrorist-Related Screening Procedures (August 27, 2004); and
- Executive Order No. 13880, on Collecting Information about Citizenship Status in Connection with the Decennial Census (July 11, 2019), 84 FR 33821 (July 16, 2019).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

ADIS is covered by and contains information from the following CBP and DHS system of records notices (SORNs):

- *DHS/CBP-005 Advance Passenger Information System (APIS)*: This SORN covers the required advance submission of passenger and crew information from air and sea carriers and private aircraft, and any other forms of passenger transportation, including rail, which is mandated or provided on a voluntary basis.
- *DHS/CBP-007 CBP Border Crossing Information (BCI)*: This SORN covers the collection of border crossing information regarding persons entering and (if applicable) exiting the United States.
- *DHS/CBP-011 U.S. Customs and Border Protection TECS*: This SORN covers the collection of the enforcement, inspection, and intelligence records relevant to the

[25] 42 U.S.C. § 1383(f).

anti-terrorism and law enforcement mission of CBP and other federal agencies that use TECS. The purpose of this system is to track individuals who have violated or are suspected of violating a law or regulation that is enforced or administered by CBP, to provide a record of any inspections conducted at the border by CBP, to determine admissibility into the United States, and to record information regarding individuals, firms, and organizations to whom DHS or CBP has issued detentions and warnings.

- *DHS/CBP-016 Non-Immigrant Information System (NIIS)*: This SORN covers the collection of arrival and departure information collected from foreign nationals entering and departing the United States, including on such forms as the I-94/I-94W or through interviews with CBP officers.[26]
- *DHS/CBP-021 Arrival and Departure Information System (ADIS)*:[27] This SORN covers the storage and use of biographic, biometric indicator, and encounter data consolidated from various systems on aliens who have applied for entry, entered, or departed the United States.
- *DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records:*[28] This SORN covers the collection of information related to transactions involving an individual as he or she passes through the U.S. immigration and inspection processes.
- *DHS/ICE-001 Student and Exchange Visitor Information System (SEVIS)*: This SORN covers the maintenance of information on non-immigrant students, exchange visitors, and their dependents admitted to the United States under an F, M, or J class of admission, as well as their school or exchange program sponsors.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

ADIS received a three-year Authority to Operate on September 11, 2019, which expires September 11, 2022. A System Security Plan was completed for ADIS on October 7, 2011, and is compliant with the National Institute of Standards and Technology (NIST) Special Publication (SP) Recommended Security Controls for Federal Information Systems (NIST SP 800-53), as well

[26] Certain information populated in the I-94W may come from the Electronic System for Travel Authorization, which is covered under DHS/CBP-009 Electronic System for Travel Authorization (ESTA), 81 FR 60713 (September 2, 2016).
[27] DHS/CBP-021 Arrival and Departure Information System, 80 FR 72081 (November 18, 2015).
[28] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (November 21, 2013).

as the DHS National Security Sensitive Systems Handbook and Policy Directive 4300A, version 5.5.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Consistent with the retention schedules for these source systems, ADIS records are retained for 75 years to ensure the data is available throughout the life of the individual. CBP is working with NARA to develop a formal records schedule for ADIS. For information about U.S. Citizens (USCs), ADIS will remove information about specific events after 15 years in accordance with the appropriate retention schedules.[29] However, ADIS will need to maintain an indicator of the individual's identity for 75 years. This indicator will retain only enough information about a traveler to identify them as a USC for the purpose of identifying them as such again when traveling in the future. Though not an exhaustive list, data elements such as name, date of birth (DOB), and passport number would be required for accurate, automated matching. This allows ADIS to ensure that the traveler is appropriately tagged as a citizen of the United States (and filtered as such, when appropriate), and not erroneously categorized as a foreign national if a future travel event contains data that is incomplete or of poor quality.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Although some of the information in ADIS is covered by the Paperwork Reduction Act, ADIS itself does not collect information directly from the public, and there are no forms or PRA collections assigned specifically to ADIS. Specific information collections relevant to traveler information collections include:

- OMB 1651-0003 – Application to Extend/Change Non-Immigrant Status;
- OMB 1651-0009 – Petition for a Non-Immigrant Worker;
- OMB 1651-0023 – Application to Register Permanent Residence or Adjust Status;
- OMB 1651-0040 – Form 1-765 Worksheet (for employment authorization);
- OMB 1651-0082 – Application to Replace Permanent Resident Card;
- OMB 1651-0088 – Passenger and Crew Manifest for Passenger Flights;
- OMB 1651-0095 – Notice of Appeal or Motion;

[29] DHS/CBP-007 Border Crossing Information, 81 FR 89957 (December 13, 2016).

- OMB 1651-0103 – Passenger List/Crew List; and
- OMB 1651-0111 – Arrival and Departure Record, Nonimmigrant Visa Waiver Arrival/Departure, and Electronic System for Travel Authorization (ESTA) (I-94 and I-94W).

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

ADIS contains data about people who: apply for a U.S. visa; apply for admission to the United States at an official port of entry; extend, change, or adjust their immigration status; depart the United States; or are apprehended by border or immigration authorities. The types of information stored in ADIS include:

Biographic Data:

- Full name;
- Date of Birth (DOB);
- Social Security number (SSN);[30]
- Citizenship (at time of event as well as naturalization, if any);
- Nationality;
- Gender;
- Country of residence;
- Country of birth;
- Travel document information (type, number, country, and date of issuance);
- E-mail address;
- Driver's license number;
- Vehicle identification number;
- License plate number;
- Occupation;

[30] ADIS stores and maintains SSNs sent by source systems.

- TECS Watch List Hit Flag;
- Federal Bureau of Investigation National Crime Information Center Watch List Flag; and
- Benefit or immigration information, such as:
    - Alien Registration Number (A-Number)
    - DOS visa information from IDENT
    - USCIS benefit information
    - DHS apprehension indicator information from IDENT
    - Benefit receipt number or relevant information such as SEVIS ID, SEVIS status, and I-94 Number

Travel Data:

- Airplane carrier code and flight number;
- Vessel port and name;
- Passenger Name Record (PNR) locator number;
- Arrival and departure information;
- U.S. destination address;
- Passenger status;[31]
- Class of admission;
- Admit until date;
- Passport and/or visa information and inspector comments; and
- Admission (I-94) Number.

Biometric Indicator Data:[32]

- Fingerprint Identification Number (FIN);[33]

[31] A passenger's mode of transportation including, but not limited to: pedestrian, crew, vehicle, on board the vessel, and not on board the vessel.
[32] The biometric indicator data fields are associated with biometric captures in the IDENT system to provide a unique identifier.
[33] ADIS does not contain fingerprint images. Fingerprint images are assigned an identifier, which is housed in ADIS; the images themselves reside in IDENT.

- Encounter Identification Number (EID);[34]
- Apprehension Type Code;
- Biometric Facial Indicator (indicating whether IDENT has a facial image stored or not);
- Biometric Indicator[35] (Y/N);
- Biometric Watch List Hit Flag; and
- Reason Fingerprinted.

Vetting Data:

CBP Automated Targeting System (ATS) – Unified Passenger (UPAX):[36] as a part of the Enhanced Overstay Validation and Biographic Exit effort, CBP uses UPAX to vet potential visa and non-visa overstay candidates based on supporting data available in multiple CBP systems. ADIS generates overstay leads based on information from source systems, which are then sent to UPAX and enriched with border crossing information,[37] SEVIS immigration and benefit information, and I-94 information.[38] UPAX prioritizes the list using targeting rules and then sends the remaining viable overstay list to ICE in an automated process. Any changes to ADIS based on this would be from feedback from ICE and usually regard data from CLAIMS or SEVIS.

2.2 What are the sources of the information and how is the information collected for the project?

ADIS does not collect information directly from individuals. Rather, the source systems listed above and in the Appendices send biographic and biometric information to ADIS in timeframes ranging from near-real time to daily updates. DHS components supply data to ADIS from their source systems that collect the information directly from individuals at Ports of Entry (POEs); from passenger manifests; through visa, passport, or benefit applications; or through certified schools or designated sponsors who input information into SEVIS that is sent directly to ADIS. DHS collects the source system data as described below. Additionally, the appendices to this PIA further discuss system and information connections.

---

[34] The EID is a unique number associated with an individual event (encounter) in which the individual's fingerprints are captured. Again, no fingerprint images are stored in ADIS.
[35] The biometric indicator field is used to show whether an event was confirmed with biometric data as opposed to solely biographic data.
[36] *See* DHS/CBP/PIA-006(e) Automated Targeting System (January 13, 2017), *available at* https://www.dhs.gov/privacy.
[37] Border crossing information housed within TECS is covered by DHS/CBP-007 Border Crossing Information, 81 FR 89957 (December 13, 2016), and DHS/CBP-016 Non-Immigrant Information System, 80 FR 13398 (March 13, 2015).
[38] I-94 information housed within TECS is covered by DHS/CBP-016 Non-Immigrant Information System, 80 FR 13398 (March 13, 2015).

CBP TECS

Information that TECS[39] provides to ADIS is either collected directly from the individual (traveler) when he or she is entering or exiting the United States (at a POE), through flight and vessel manifests, or through other federal or foreign systems. Specifically, TECS provides:

APIS: APIS is manifest information collected by air, sea, rail, and bus carriers or private aircraft owners about passengers and crewmembers who travel to, from, or through the United States. Carriers submit information to CBP in advance of their arrival to the United States for screening purposes. Upon a traveler's arrival into the United States, a CBP Officer verifies that the data transmitted by the carrier is the same as that on the traveler's travel documents. APIS information is sent to ADIS in real time through an automated process.

TECS Border Crossing Records: Border-crossing records consist of information CBP collects from individuals during primary inspection as the individual is admitted or paroled into or exits the United States through an air, sea, or land POE. This includes CBSA implied exit records.[40] As part of the Beyond the Border Entry/Exit Program,[41] CBSA and CBP exchange entry information on individuals crossing at all automated common land border POEs to create exit records from the other country. This exchange of border crossing exit information assists Canada and the United States in matching land exit documentation to previously-held entry records. Implied exit records are also provided to ADIS.

Non-Immigrant Information System I-94/I-94W: ADIS receives information collected from the I-94/I-94W form as a record of a non-immigrant's arrival in the United States, and as a means of determining when the non-immigrant has departed from the United States. The I-94W is generated using a traveler's application through the Electronic System for Travel Authorization (ESTA),[42] which automated the I-94W form into a web application for travelers from visa waiver countries. CBP automated the I-94 form using existing collections (APIS and visa information from DOS). An individual receives an I-94/I-94W form when entering the country at the land border and is expected to return the form when departing the country, thus creating and adding confidence to the departure

[39] For more information about the TECS system, *see* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing and DHS/CBP/PIA-021TECS System: Platform, *available at* https://www.dhs.gov/privacy.
[40] Implied exit records refer to Canadian entry records that CBP takes to indicate an exit record from the United States. They are "implied" only because CBP has not officially processed them as an exit; rather, CBSA has noted them as an entry, which CBP infers to be an exit.
[41] *See* DHS/CBP/PIA-004(h) Beyond the Border Entry/Exit Program Phase III (August 12, 2016), *available at* https://www.dhs.gov/privacy.
[42] *See* DHS/CBP/PIA-007(g) Electronic System for Travel Authorization (September 2, 2016) *available at* https://www.dhs.gov/privacy, and DHS/CBP-009 Electronic System for Travel Authorization, 81 FR 60713 (September 2, 2016).

event in ADIS. ADIS will be subsuming the I-94 beginning in fiscal year 2020, as the systems have become largely duplicative.

CBP Secondary Inspections: ADIS receives certain records created during secondary inspections. CBP Secondary inspection allows CBP Officers to conduct additional research in order to verify a traveler's information without causing delays for other arriving travelers. A CBP Officer must create a secondary inspection incident record for all passengers referred by CBP Primary inspection.

USCIS ELIS, CLAIMS 3 & 4, and PCQS

USCIS uses multiple case management systems to process immigration requests. The case management system used varies by the type of immigration request. CLAIMS 3 primarily processes most domestically-filed immigration requests with the exception of naturalization, intercountry adoption, and certain requests for asylum and refugee status. USCIS ELIS also processes certain domestically filed immigration requests, as well as applications for naturalization and citizenship. CLAIMS 4 has been historically used to process applications for naturalization and citizenship, but is in the process of being decommissioned and replaced by USCIS ELIS.

ADIS receives information from both CLAIMS 3 and USCIS ELIS. In limited circumstances, ADIS also queries CLAIMS 4 via the Person Centric Query Service (PCQS) to identify if a suspected overstay has become a naturalized citizen. ADIS also provides data to PCQS via a connection to its web services.

CBP e3

CBP operates the e3 portal,[43] which serves as the CBP portal to the ICE Enforcement Integrated Database (EID) and IDENT to collect and transmit data related to law enforcement activities. e3 collects and transmits biographic, encounter, and biometric data for identification and verification of individuals encountered at the border for CBP's law enforcement and immigration mission. Previously, ADIS received apprehension data from IDENT, but this information is now received from e3.

ICE SEVIS

In addition to ADIS receiving SEVIS information through ATS-UPAX, SEVIS also sends information about the status of students and exchange visitors directly to ADIS via an automated interface.

OBIM IDENT[44]

[43] See DHS/CBP/PIA-012, CBP Portal (E3) to ENFORCE/IDENT, available at https://www.dhs.gov/privacy.
[44] IDENT is in the process of being replaced by the Homeland Advanced Recognition Technology (HART) system.

IDENT appends biometric identifiers to events captured by other source systems, and sometimes acts as a conduit for information from those systems (e.g., DOS CCD). ADIS receives the following data elements related to an individual, if available: the Fingerprint Identification Number (FIN), Encounter Identification Number (Event ID), and encounter updates (meaning a notification that another IDENT user agency has encountered the individual, which may be relevant for the purposes of verifying that individual's status). Through IDENT, ADIS receives or has received information from a number of federal agencies who collect the information through various methods, depending on their authorities and mission. These methods include:

- Directly from the individual at a port of entry (POE) or via an application for an immigration benefit;
- Indirectly, such as in the case of records shared by foreign governments according to written agreement or cooperative arrangement; or
- Directly or indirectly from the individual during a law enforcement action.

IDENT collects some data from data providers through an online application, a paper-based application, a mobile biometric device, a fixed platform, or in-person interviews. IDENT also receives latent prints from crime scene and/or another site relevant to the work of an IDENT user, such as the site of a terrorist incident. The data is then securely transmitted to IDENT, where it is used to support the DHS mission.

ADIS may receive messages from IDENT, containing information from systems such as CCD or CLAIMS, which either create a new identity or provide a status update associated with an identity. For example, an apprehension message that relates to the type of enforcement event recorded biometrically within the IDENT system could be shared with ADIS. ADIS stores data pertaining to apprehensions, but does not store derogatory information such as arrest reports or the details of an investigation. Instead, it uses the enforcement apprehension event type to determine whether a removal or law enforcement action involving custody has occurred, thus possibly closing an overstay record in ADIS.

TSA Alien Flight School Program

TSA provides ADIS with risk-based information that is used during the overstay lead-generation process. Risk-Based Performance Standard 12 (RBPS-12)[45] requires that TSA implement "measures designed to identify people with terrorist ties" for persons seeking training in the United States as an airline pilot. CBP has implemented the ADIS web service to facilitate the identification of high-risk trainees to comply with RBPS-12.

[45] 6 CFR 27.230(a) (12)(iv).

Department of State Consular Consolidated Database

The CCD is a repository of data from consular posts abroad and domestic processing centers. ADIS receives, via IDENT, information about visa applications and issuances. This assures that affected travelers are in ADIS when they arrive to the United States, assisting CBP officers with determining admissibility.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

ADIS does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

ADIS relies on matching algorithms to combine an individual's entry and exit data with information about his or her immigration status. CBP monitors the system to assess accuracy using different match rates, and performs annual maintenance to implement improvements to biographic matching. CBP continually monitors and rectifies discrepancies with identities in the system.

CBP also relies upon the source component to verify the quality of the data at the time of collection before sending it to ADIS. Additionally, ADIS intentionally receives the same data from multiple sources as a crosscheck to ensure the data is as accurate as possible. ICE Counterterrorism and Criminal Exploitation Unit (CTCEU) and ADIS analysts review the data from separate sources and compare it to the aggregated data within ADIS to determine if identities have been incorrectly merged or split, and then recommend corrective action to CBP based on their findings. Analysts make the corrections as warranted.

CBP uses custom and open source algorithms, and has implemented multiple technology upgrades to matching to ensure accuracy of the data. Individuals who believe that the data held on them in a source system is inaccurate may submit a redress request for a review and correction of that inaccurate data. For more information refer to Section 7.0 of this PIA on redress.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of overcollection of United States citizen information when that information is of minimal use in determining overstays.

Mitigation: This risk is partially mitigated. ADIS allows CBP to share travel information about USCs without granting access to TECS, which is a law enforcement system containing a variety of derogatory and other information of similar sensitivity. ADIS's person-centric design combined with its unique filtering capabilities allow CBP to share data with stakeholders with

more complex access controls. For example, if there was 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—whether via the ADIS web portal, web services, or other methods of sharing data. 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.

Privacy Risk: There is a risk that the ADIS matching algorithm will result in a false match, resulting in either an adverse determination related to an immigration benefit, or in CBP's inability to appropriately take action on an overstay or other violation.

Mitigation: CBP mitigates this risk by taking steps to corroborate all information before taking an adverse action. If ADIS matching algorithms generate an overstay alert, the CBP Officer investigating the case will review the match and ensure that the record pertains to the correct individual. No action is taken based solely on ADIS (or any other system-generated) alerts.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

ADIS information assists CBP and other agencies in identifying and contacting individuals who have overstayed the terms of their admission into the United States. Additionally, with the ingestion of U.S. citizen information, ADIS will operate as a single system for travel and immigration information that will limit the disclosure of law enforcement sensitive information. Once ADIS creates a person-centric record based on data from the source systems, it tags the record for inclusion in one of five populations: non-U.S. persons, Lawful Permanent Residents (LPRs) and other non-citizen U.S. persons, Special Protected Classes, refugees and asylum applicants, and U.S. citizens (naturalized or native-born). Persons whose status changes over time remain appropriately tagged in accordance with any changes to their status. USCIS provides a list of individuals protected by 8 U.S.C. § 1367 (Special Protected Classes); ADIS tags these populations if the provided information matches to an ADIS record. Furthermore, ADIS has internal algorithms designed to identify any Special Protected Classes, refugees, applicants for asylum, and U.S. citizens.

ADIS provides status information to partners and source systems as outlined below:

- Travel history and person details to USCIS systems (including ELIS, Person Centric Query Service, E-Verify, and the Systematic Alien Verification for Entitlements program);

- I-94 travel and departure closure messages to TECS to update traveler records; ADIS information is used for updates to the public I-94 website, allowing travelers to view their status of admission and whether they have overstayed;
- Un-vetted overstays and ICE Counterterrorism and Criminal Exploitation Unit (CTCEU) leads to CBP's Automated Targeting System (ATS);
- Student travel events to ICE (SEVIS);
- Travel history and status change events to the Federal Bureau of Investigation (FBI);
- Travel history and person details to the DOS Consolidated Consular Database (CCD);
- I-94 travel and travel history to the Department of Commerce;
- Travel history and person details to the Social Security Administration; and
- Travel history, status change events, and person details to the Department of Defense and Intelligence Community.

ADIS receives biographic and biometric indicator data from other DHS systems to create a person-centric account of entries into and exits from the United States, as well as probable immigration status. CBP, DHS components, and other federal agencies use ADIS in addition to other sources of information as part of their official responsibilities to:

- Eliminate falsely-identified overstays for dual citizens traveling with a foreign passport;
- Facilitate identification and investigations of individuals who may have violated immigration statute and regulations, including their terms of admission into the United States;
- Assist with determining eligibility for U.S. visa or immigration benefits, including entry into the United States;
- Assist in the investigation of individuals who may be subjects of interest for national security, law enforcement (including prosecution), immigration and border management, and intelligence purposes;
- Assist with conducting background checks on persons with international travel seeking to enter federal facilities;
- Assist with identifying instances of benefit fraud;

- Generate statistical reports on travel to and from the United States, as well as reporting on overstay rates by country; provide associated testing, training, management reporting, planning, and analysis, and for other administrative purposes; and
- Share information with partners without oversharing law enforcement sensitive or protected information.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

ADIS does not conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly. However, other federal agencies in receipt of ADIS data may use it as a source in other data mining activities to support analysis performed for national security, law enforcement, immigration and border management, intelligence purposes, and other DHS mission-related functions. Any use of the data for these purposes must be approved by the data owner and supported by the required documentation (including SORNs, PIAs, and MOUs for non-DHS entities).

3.3 Are there other components with assigned roles and responsibilities within the system?

ADIS allows users from other agencies to query ADIS. CBP only provides read-only access to ADIS records. Appendices A and B fully discuss the roles of other users in ADIS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: Because a large number of users access ADIS in support of their missions, there is a privacy risk that ADIS data may be used in a manner inconsistent with the original collection.

Mitigation: This risk is partially mitigated. The primary goal of ADIS is to identify aliens who may be in violation of the terms of their entry into the United States; a variety of other Federal Government agencies within and outside of DHS have a vital interest in this information in accordance with their authorities. CBP primarily shares ADIS data with DHS components in support of the missions for which ADIS was initially developed. Further, CBP ensures that outside agencies requesting access to ADIS information are authorized to request the data for the fulfillment of their duties; access requires information sharing agreements that outline the use limitations. CBP ensures compliance with agreements through audit logs, automatic data changes

and deletions, stakeholder engagement, and other mechanisms. ADIS information that is shared outside of DHS is shared pursuant to the routine uses listed in the relevant source system SORNs, which serve to place limitations on the sharing of data and provide notice to the public of these uses.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Generally, the collecting organization provides notice at the point of collection that the information may be shared with other federal, state, local, and foreign government agencies and authorized organizations following approved routine uses described in the associated published SORNs. This PIA provides new notice that CBP is now using ADIS to retain USC information collected by other systems. Additionally, this PIA provides notice to the public that the information they provide to other systems may then be shared with other federal agencies or systems, such as ADIS. When applicable, Privacy Act statements are provided to individuals at the time of the collection or through the websites of the data-collecting DHS components.

CBP: For its collection of border crossing and inspection data, CBP provides notice through its PIAs and SORNs, and on forms such as the I-94, ESTA applications,[46] and other forms that are required of individuals seeking to enter the United States. CBP has posted signs in POEs, which provide notification of the forms and steps required to enter the United States. Additionally, CBP may provide handouts to individuals during secondary inspection regarding any additional information required, or when requested.

USCIS: USCIS provides notice to individuals by requiring applicants to sign a release authorization on the benefit application or petition they are submitting. USCIS forms feature Privacy Act statements outlining USCIS' authorities and purpose for collecting the information, as well as information on routine uses and notice of any consequences for failing to provide the information.

ICE: ICE provides notice to SEVIS applicants by publishing the SEVIS PIA, and its subsequent update, and the SEVIS SORN.[47] Additionally, the certified school or designated

[46] Notice is also provided on the ESTA website, *available at* https://esta.cbp.dhs.gov/esta/application.html?execution=e1s1.
[47] *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).

sponsor may provide notice to the individual prior to submitting information into SEVIS, which then submits that information to ADIS.

TSA: TSA provides notice of the security threat assessment requirement for all candidates seeking recurrent flight training via a statement posted on www.flightschoolcandidates.gov. A Privacy Act statement is provided to each candidate. Additionally, TSA published the Alien Flight Student Program PIA and the applicable SORN[48] for additional notice. The notice also informs candidates that the collection of the information is voluntary, but those who decline to provide it will not be eligible for the requested flight training. Candidates who are not willing to provide the required information may choose not to apply for flight-training or withdraw their application.

OCSO: OCSO collects information directly from an individual, or his or her representative, who requests to visit DHS facilities. OCSO provides the individual notice in written or verbal form at the time PII is collected. The individual is also advised that DHS will use this information to vet him or her to determine if access may be granted to a DHS facility. A Privacy Act statement is contained on the data collection tool or email message provided to the individual or the individual's representative. Additionally, OCSO published the Foreign Access Management System PIA, and notice is also provided through the Facility and Perimeter Access Control and Visitor Management SORN.[49]

DOS: The Department of State has published a PIA for the Consular Consolidated Database (CCD) and a Visa Records SORN,[50] which provide notice to the public of this information collection; both are available on the DOS website.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Information provided by the individual is a requirement for receiving an immigration benefit (such as a U.S. visa), gaining entry into the United States, or obtaining other government benefits. CBP considers crossing the border to be a voluntary action and as such, individuals must comply with the rules and regulations CBP enforces. Once an individual has provided his or her information, there is no opportunity to consent to or refuse the use of this data for any of these purposes.

---

[48] *See* DHS/TSA/PIA-026 Alien Flight Student Program (AFS) (July 28, 2014), *available at* https://www.dhs.gov/privacy, and DHS/TSA-002 Transportation Security Threat Assessment System, 79 FR 46862 (August 11, 2014).

[49] *See* DHS/ALL/PIA-048(a) Foreign Access Management System (FAMS) (December 12, 2014), and DHS/ALL-024 Facility and Perimeter Access Control and Visitor Management, 75 FR 5609 (February 3, 2010), *available at* https://www.dhs.gov/privacy.

[50] *See* Privacy Impact Assessment, Consular Consolidated Database (July 17, 2015), *available at* https://foia.state.gov/_docs/PIA/ConsularConsolidatedDatabase_CCD.pdf, and DOS Visa Records SORN, 77 FR 65245 (October 25, 2012).

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that individuals may not be aware at the time of collection that the information they are providing will be stored in ADIS.

Mitigation: The collecting agency provides notice at the point of collection that the information may be shared with other federal, state, local, and foreign government agencies and authorized organizations following approved routine uses described in the associated published SORNs. In addition, CBP mitigates this risk through publication of this PIA, as it serves as public notice of sharing information by DHS components and other agencies to ADIS. Further, some collecting components also provide notice through their published PIAs that the information collected may be shared with ADIS. For example, CBP states in the APIS PIA[51] that certain information from APIS is shared with ADIS.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

For non-USC information, CBP is proposing a retention schedule of 75 years, consistent with the retention schedules for ADIS source systems. For information on USCs, CBP will retain source system underlying biographic information for 15 years, but will maintain a basic indicator, solely for the purpose of tagging that traveler as a USC, for 75 years. CBP is working with NARA to develop a formal records schedule.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that CBP will store U.S. citizen data for longer than necessary in ADIS, thereby increasing the risk of unauthorized access, use, and loss of the data.

Mitigation: This risk is partially mitigated. Retention of border crossing data for USCs is limited to 15 years, pursuant to the Border Crossing Information SORN.[52] Any ADIS records that relates to a USC who has not been properly identified and tagged would be retained according to the ADIS system schedule, which is 75 years. This risk of over-retention is mitigated by the fact that CBP aggressively monitors ADIS for data pertaining to USCs, and any record pertaining to USCs is flagged as such. CBP continuously updates and tests ADIS tagging functionality to improve its filtering capabilities and reduce the risk of unnecessary retention of records. However, ADIS retains a USC indicator, which includes name, date of birth (DOB), and passport number, that

[51] *See* DHS/CBP/PIA-001 Advance Passenger Information System (APIS), *available at* https://www.dhs.gov/privacy.
[52] DHS/CBP-007 Border Crossing Information, 81 FR 89957 (December 13, 2016).

denotes that person is a USC after the other information associated with them is deleted from ADIS after 15 years.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

CBP shares information stored in ADIS with appropriate federal, state, local, tribal, foreign, or international government agencies, as part of normal agency operations. DHS also has information sharing agreements with external agencies (including intelligence agencies) that establish the rules for using ADIS information. Partner agencies use the information for purposes compatible with the purpose of the original collection and their authorities. A list of partner agencies with access to ADIS data is included in Appendix B of this document.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

As ADIS is a data aggregator, any information shared outside of ADIS must be done in compliance with the SORNs governing the source system information within ADIS. As outlined in the various source system SORNs noted in section 1.2, CBP uses ADIS for a variety of traveler compliance purposes including pre-entry, entry, status management, and exit tracking of immigrants and non-immigrants, and to determine whether individuals have maintained legal status and facilitate investigations of the status of individuals who remain in the United States beyond their authorized stay, and permit non-law enforcement queries of CBP travel data. Any external sharing from the ADIS system is reviewed for compatibility with the source system SORNs that govern the impacted data elements. Generally, most source system SORNs have the following routine uses that cover the most frequent types of ADIS data sharing, although the routine use letter may vary:

- Routine Use G states that CBP can share ADIS data with appropriate federal, state, tribal, local, international, or foreign law enforcement agencies or other appropriate authorities charged with investigating or prosecuting a violation of or enforcing or implementing a law, rule, regulation, or order, when CBP believes the information would assist enforcement of applicable civil and criminal laws, and such disclosure is proper and consistent with the official duties of the person making the disclosure.
- Routine Use H states that CBP can share ADIS data with appropriate federal, state, local, tribal, foreign, or international governmental agencies seeking information

on the subjects of wants, warrants, or lookouts, or any other subject of interest, for purposes related to administering or enforcing the law, national security, or immigration, when consistent with a DHS mission-related function as determined by DHS.

- Routine Use K states that CBP can share ADIS data with federal, state, local, tribal, foreign or international government intelligence or counterterrorism agencies or components when DHS becomes aware of an indication of a threat or potential threat to national or international security, or when such use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.
- Routine Use L states that CBP can share ADIS data with federal, state, and local government agencies for any legally mandated purpose in accordance with an authorizing statute and when an approved Memorandum of Agreement or Computer Matching Agreement (CMA) is in place between DHS and the agency.

6.3 Does the project place limitations on re-dissemination?

Yes. DHS information sharing agreements address limitations on re-dissemination. Partner agencies are required to first notify CBP and request permission before onward sharing.

DHS Policy for Internal Information Exchange and Sharing allows information to be shared within DHS whenever the requesting component has an authorized purpose for accessing the information in the performance of its mission.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Most disclosures of CBP data for Freedom of Information Act (FOIA), Privacy Act, or routine use purposes pertain to source system data. Because ADIS consists of data aggregated from source systems, it is less frequently implicated in responding to requests for information. More commonly, ADIS data is shared outside the Department pursuant to information sharing agreements and via the methods listed in the overview. ADIS tracks all automated data exchanges and bulk data extracts, and ADIS Web Services has system logs for automated transactions. Because ADIS does not automatically log manual data extracts, CBP applies the DHS policy for managing computer readable extracts containing sensitive personally identifiable information.[53]

[53] For more information, please s*ee* https://www.dhs.gov/sites/default/files/publications/4300A-Handbook-Attachment-S1-Managing-CREs-Containing-SPII.pdf.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that since ADIS is not the original source of data collection, information may be updated by the source system after it is shared with an external agency, and that agency's information will no longer be complete, timely, and accurate.

Mitigation: Although CBP relies on the accuracy of the source systems and the ability of the collecting component to verify the quality of the data before sending it to ADIS, the system itself has a number of capabilities that help ensure the accuracy of the data. Data from source systems are refreshed in near real-time, with the one exception of a daily refresh from USCIS's CLAIMS. Additionally, ADIS may intentionally receive the same data from multiple sources as a cross-check so that the system can ensure the data is as accurate as possible. When an error is identified, source systems as well as users in the field may send corrections to ADIS, which ADIS implements upon receipt. Corrective actions to ADIS are made through I-94 update messages to correct manual entry error, or through requests presented to users with the appropriate permissions for updating and correcting records. Partners receiving ADIS data extracts receive corrected records automatically, since they only receive records that have been changed or updated.

Privacy Risk: Because ADIS contains information linked to Special Protected Classes of aliens, there is a risk that their information will be shared without the appropriate protections.

Mitigation: ADIS contains information related to aliens whose information is generally prohibited from disclosure to agencies outside DHS, the Department of Justice, and DOS unless the disclosure is within certain delineated exceptions (for example, to a law enforcement official for a legitimate law enforcement purpose). ADIS's tagging capability ensures that CBP is able to identify records pertaining to Special Protected Classes. CBP does not share this information with agencies who do not meet the exemptions described above. For those agencies that may receive special protected class records, CBP articulates the requirement for protection of this information in its information sharing agreement.

Once a person-centric record is created in ADIS based upon records from the source system, the record is tagged for inclusion in one of five populations: non-U.S. persons, Lawful Permanent Residents (LPRs) and other non-citizen U.S. persons, Special Protected Classes, refugees and asylum applicants, and U.S. citizens (naturalized or native-born). U.S. citizens are identified by the presence of a U.S. passport or naturalization certificate in their travel records; these records are then screened for verification. USCIS provides a list of individuals associated with Special Protected Classes and these populations are tagged if the information provided matches to an ADIS record.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Because the information in ADIS consists of data provided by other source systems, information responsive to access requests may be obtained from the source system of records. Information on these systems of records may be found in the SORNs listed in Section 1.2 of this PIA. In addition to the FOIA and Privacy Act request processes described in Section 7.2, individuals can access information from their I-94 form admission record to verify immigration status or employment authorization, the record number, and other admission information; individuals may access that information through CBP's public website.[54]

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals seeking notification of and access to records contained in ADIS, or seeking to contest its content, may submit a FOIA or Privacy Act request to CBP at https://foia.cbp.gov/palMain.aspx, or by mailing a request to:

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
FOIA Division
1300 Pennsylvania Avenue, NW, Room 3.3D
Washington, D.C. 20002
Fax Number: (202) 325-1476

Requests for information are evaluated to ensure that the release of information is lawful; will not impede an investigation of an actual or potential criminal, civil, or regulatory violation; and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

All FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process.

Persons who believe they have been improperly denied entry, refused boarding for transportation, or identified for additional screening by CBP may submit a redress request through DHS Traveler Redress Inquiry Program (TRIP). DHS TRIP is a single point of contact for persons who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs—like airports, seaports, and train stations or at U.S. land borders.

[54] *Available at* https://www.cbp.gov/travel/international-visitors/i-94-instructions.

Through DHS TRIP, a traveler can request correction of erroneous data stored in DHS databases through one application. Individuals can file a DHS TRIP redress request at http://www.dhs.gov/dhs-trip or by mail at:

DHS TRIP
601 South 12th Street, TSA-901
Arlington, VA 22202

7.3 How does the project notify individuals about the procedures for correcting their information?

Individuals are advised of the procedures for correcting their information in this PIA, all of the source system SORNs noted in Section 1.2, and on the DHS and CBP public-facing redress websites.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that individuals, particularly non-U.S. persons, may not know how to access, correct, or amend inaccurate information about themselves in ADIS.

Mitigation: This PIA and the SORNs of source systems provide notice of the procedures for access to and correction or amendment of records. DHS TRIP, as outlined above, provides notice of the redress process through a website that facilitates the submission and processing of redress requests. Any individual can request access to or correction of his or her PII regardless of his or her nationality or country of residence.

Privacy Risk: There is a privacy risk that non-U.S. persons may not have access to or be able to amend their records at all.

Mitigation: This risk is partially mitigated. This PIA and the ADIS SORN describe how individuals can make access requests under the Freedom of Information Act or the Privacy Act. Redress is available for U.S. citizens and Lawful Permanent Residents through requests made under the Privacy Act as described above. U.S. law prevents DHS from extending Privacy Act redress to individuals who are not U.S. citizens, Lawful Permanent Residents, or the subject of covered records under the Judicial Redress Act. To ensure the accuracy of CBP's records, CBP may permit access and amendment, regardless of citizenship, on a case-by-case basis, consistent with law.

In addition, providing individual access and/or correction of ADIS records may be limited for law enforcement reasons as expressly permitted by the Privacy Act. Permitting access to the records contained in ADIS, regardless of a subject's citizenship, could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the

individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, or to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

CBP reviews all requests for access to and correction of records, including from non-U.S. persons. When CBP becomes aware of an inaccurate record, it will make corrections whenever possible in the interest of maintaining the accuracy of the data in its systems.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

ADIS secures its data by complying with the requirements of DHS information technology security policy, particularly the DHS Sensitive Systems Policy Directive 4300A. This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules. CBP periodically evaluates ADIS to ensure that it complies with these security requirements.

Additionally, the ADIS Web application has four primary user roles that dictate function authorization: ADS_Read-Only, ADS_User, ADS_Update, and ADS_Admin. ADS_Update and ADS_Admin have two additional functions that cover administrative actions relating to data integrity updates and function authorization relating to administrative rights. Both roles are maintained and restricted to CBP and ICE.

ADIS provides audit trail capabilities in order to monitor, log, and analyze system transactions as well as actions and system accesses of authorized users. CBP periodically conducts reviews for compliance within the program and between external partners to ensure that the information is used in accordance with the stated acceptable uses documented in the MOU, SORN, sharing agreements, and other technical and business documentation.

Because ADIS contains data from a variety of sources, collected for a variety of uses, it is necessary to institute controls so that only those individuals making the appropriate use of the data are able to access that data. ADIS has a robust set of access controls, including role-based access and interfaces, which limit individuals' access to the appropriate discrete data collections. Misuse of data in ADIS is prevented or mitigated by requiring that users conform to appropriate security and privacy policies, follow established rules of behavior, and are adequately trained regarding the security of their systems. CBP also performs a periodic assessment of physical, technical, and administrative controls to enhance accountability and data integrity. External connections must be

documented and approved with both parties' signatures in an Information Security Agreement (ISA), which outlines controls in place to protect the confidentiality, integrity, and availability of information being shared or processed.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

DHS employees and contractors who access ADIS are required to complete annual privacy and security awareness training. For users outside of DHS, privacy and ADIS system training is provided by the ADIS Business Owner.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

CBP has documented standard operating procedures to determine which users may access ADIS. The minimum requirements for access to ADIS are documented in information sharing arrangements between and among DHS and specific stakeholders, and in security, technical, and business documentation. In order to access ADIS, all employees and contractors must have a favorably adjudicated background investigation required by their employing agency to receive access to sensitive but unclassified systems. All investigations must be in-scope at the time that access is granted and remain in-scope for the duration of the access. Individuals must have demonstrated a need to know the information based on their job responsibilities and verified by a supervisor, and must participate in security and privacy awareness training.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All information sharing and information sharing agreements must be reviewed and approved through an internal CBP process, which includes a review by the policy and privacy teams, as well as legal counsel. Then it is submitted to CBP leadership as appropriate for final review and approval.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk: There is a privacy risk that individuals may have unauthorized access to the information maintained in ADIS.

Mitigation: To mitigate this risk, CBP employs role-based access controls so that authorized users have only the access they need in order to perform their functions. Only users with a need to know may access ADIS; together with the principle of least privilege, a CBP ADIS

Business Owner determines what features in ADIS the user will access. Only System Administrators and users with update roles can access and change fields in the database. Additionally, all users of ADIS user accounts must conform to appropriate security and privacy policies, follow established rules of behavior, and be adequately trained regarding the security of their systems. CBP also performs a periodic assessment of physical, technical, and administrative controls to enhance accountability and data integrity. In addition, the CBP Privacy Office may conduct privacy evaluations of systems to ensure that the system is being managed in accordance with DHS privacy policy and published privacy notices.

Responsible Officials

Michael J. Gorman, Director
Mission Systems & Data Services
Office of Field Operations
U.S. Customs and Border Protection
Department of Homeland Security

Debra L. Danisek, CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection
Department of Homeland Security

Approval Signature

[Original signed and on file with the DHS Privacy Office]

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Appendix A

Authorized DHS ADIS Users

CBP: CBP uses ADIS during the immigration inspection process (the interview process at the border where CBP determines whether to admit or parole the individual into the United States). ADIS is used at POEs to establish travel patterns, including for the purpose of determining if an individual previously overstayed his or her terms of admittance, and to otherwise assist in determining if the individual is admissible to the United States. CBP Officers also use ADIS to search and run reports at POEs. ADIS is integrated with the National Targeting Center through the Unified Passenger (UPAX) system, which enables automated and manual queries to support vetting and targeting operations. Analysts in the CBP Office of Field Operations ADIS Vetting Unit (AVU) have ADIS read/write user accounts to help determine the status of lawfully admitted aliens that depart beyond their period of authorized stay (i.e., "overstays"). CBP analysts consolidate travel and immigration history from different sources and create a complete travel and immigration history of an individual. All CBP ADIS users outside of the AVU and ADIS business/system owners have read-only access.

USCIS: USCIS uses the information in ADIS to assist in granting or denying an individual's immigration benefits. For example, if an individual previously overstayed his or her authorized period of admission, he or she may not be eligible to receive benefits. USCIS also uses the information to verify an individual's eligibility to be in the country for employment purposes. USCIS uses the overstay indicator and travel results from ADIS queries to generate a compliance status with other government entities outside of DHS. USCIS uses the Person Centric Query System (PCQS) for benefit adjudicators to assist in granting or denying an individual's benefits and detecting fraud. Approved stakeholders can access ADIS data through PCQS. USCIS users have read-only access.

ICE: ICE analysts and officers use ADIS accounts to help determine the status of lawfully admitted aliens that remain in the United States beyond their period of authorized stay (i.e., "overstays") who may pose national security or public safety threats. Through ADIS user accounts, analysts query other federal immigration systems to validate a potential overstay. ICE also uses ADIS user accounts to review the entry and exit of aliens who may have violated their admission status. Information from ADIS is sent to ICE for further investigation of these individuals. Additionally, ICE analysts and officers query ADIS in support of criminal and administrative investigations under their jurisdiction. Furthermore, ICE uses ADIS overstay and non-overstay data extracts for reporting purposes. Information exchanged for overstay vetting purposes is also provided to ICE Enforcement and Removal Operations (ERO). ICE users have read-only access.

OCSO: OCSO uses ADIS user accounts to assist in confirming the identity of individuals who request access to DHS facilities, information, and programs or who come in contact with DHS

personnel. This supports the vetting process by providing for more accurate identity verification. OCSO then notifies the submitting components of the vetting process results. OCSO users have read-only access.

OBIM: OBIM may use ADIS, in conjunction with IDENT, to confirm an individual's identity for research and analytical support of requests for information for specific subjects or persons of interest or admission status or for redress. OBIM users have read-only access.

Office of Immigration Statistics (OIS): OIS uses ADIS data extracts of overstays and other travel populations to assist with statistical reports. The primary data export exchange is associated with validation of country specific overstay rates presented in the DHS Annual Entry/Exit Overstay Report, which DHS provides to Congress. In addition, OIS has read-only access to the ADIS-R reporting environment.

TSA: TSA requests information from ADIS, through Web Services or a two-way connection and manual extracts, to vet Alien Flight Student Program (AFSP) applicants against the ADIS database. Its mission is to detect and identify AFSP applicants who are in violation of their overstay status. TSA provides the results to ICE CTCEU to take appropriate immigration enforcement action. TSA users have read-only access.

Appendix B

Authorized ADIS Users Outside of DHS

The U.S. Department of State: DOS accesses ADIS to retrieve visa, passport, immigration, naturalization, and citizenship records as part of its decision-making process in adjudicating visa applications. Prior to coming to the United States, many individuals are required to obtain a visa. The arrival and departure information of individuals traveling to and from the United States is useful in determining an individual's eligibility for receiving or renewing a visa. Consular Affairs (CA) also uses aggregated ADIS data to identify trends regarding overstays, visa fraud, and other similar activities. ADIS has been supporting DOS since 2003. DOS users have read-only access.

DOS searches ADIS through the Consolidated Consular Database (CCD). Communication between ADIS and CCD is an automated process using ADIS Web Services technology in which CCD submits requests to ADIS, and in response, ADIS replies to CCD with travel history and status information as defined by the search parameters. Overstay trend analysis is performed through manual data runs by ADIS staff.

Applicable ADIS SORN (2015) Routine Uses G, H.

Memorandum of Agreement between DOS and DHS for Enhanced Border Security signed January 11, 2005.

U.S. Department of Justice, FBI: ADIS provides information to the Foreign Terrorist Tracking Task Force (FTTTF), National Instant Criminal Background Check System (NICS), and other employees of the FBI to: assist in mitigating potential national security risks and threats, prevent unauthorized aliens from obtaining firearms, and otherwise support the FBI's missions as permitted by law. FTTTF accesses ADIS directly through user accounts and also receives a feed of ADIS information, which is automatically downloaded by FTTTF on a daily basis. The data provided to FTTTF is used to assist the agency with locating or detecting the presence of individuals who may pose a risk to national security. FTTTF makes ADIS data available to end users through the FBI's Data Integration and Visualization System, which allows appropriately trained and authorized personnel throughout the country to query for information of relevance on investigative and intelligence matters. ADIS has supported FTTTF since 2004. DOJ users have read-only access.

ADIS provides NICS with records about aliens suspected to be lacking a valid immigration status, as the ability of the NICS to determine quickly and effectively whether an individual is prohibited from possessing or receiving a firearm depends on the completeness and accuracy of the information made available to it by federal, state and tribal authorities. Pursuant to 18 U.S.C. § 922(g)(5), any person "who, being an alien, (A) is illegally or unlawfully in the United States;

or (B) except as provided in subsection (y)(2), has been admitted to the United States under a nonimmigrant visa (as that term is defined in section 101(a)(26) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(26))" is prohibited from shipping, transporting, possessing, or receiving firearms under federal firearms laws.

Applicable ADIS SORN (2015) Routine Uses G, H, K.

Memorandum of Agreement between DHS and DOJ/FBI for the purpose of sharing US-VISIT and SEVIS information signed February 10, 2005.

The U.S. Intelligence Community (IC): DHS shares ADIS information with certain elements of the IC in support of the Department's mission to protect the United States from potential terrorist activities. In order to enhance information sharing, the President issued Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans* (October 27, 2005), which provides that the head of each agency that possesses or acquires terrorism information shall promptly give access to that information to the head of each other agency that has counterterrorism functions. Likewise, the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004,[55] as amended, places an obligation on U.S. Government agencies to share terrorism information with the IC.

For this reason, and to enhance our nation's security, DHS shares data with certain members of the IC. For example, CBP shares data with the National Counterterrorism Center (NCTC), which serves as the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support. CBP shares information with the IC in order to support counterterrorism activities, intelligence, and other IC activities and to identify terrorism information within DHS data. This information sharing aligns with DHS's mission to prevent and deter terrorist attacks and protect against and respond to all threats and hazards to the Nation.

Additionally, certain elements of the IC may conduct searches of ADIS for matters relating to national security. ADIS data may be shared through system interfaces or through data extracts from the ADIS database. Upon request, the ADIS team may respond to ad hoc requests for information from the IC to provide information related to subjects of wants, warrants, or lookouts, or any other subject of interest. ADIS information is only shared for purposes related to administering or enforcing the law, national security, and immigration or intelligence purposes consistent with the ADIS SORN.

All inter-agency agreements with the IC outline a number of safeguards to ensure that data is being used solely for the purposes explicitly stated in the agreement, PIAs, and SORN. DHS requirements limit the amount of time the information is maintained by the IC, ensure proper

[55] Pub. L. 108-458 (December 17, 2004).

information technology security is in place during and after ADIS data transmission, delete information when it is not needed, and require training for the user in interpreting ADIS data and on handling and safeguarding the PII contained in ADIS. Lastly, there are routine reports and audits completed to monitor the use of ADIS data.

The DoD conducts full-spectrum counterintelligence activities in support of commanders and joint military activities to protect forces, secrets, and technologies by detecting, identifying, neutralizing, and exploiting foreign intelligence services and international terrorist threats. ADIS data supports this mission in counterintelligence analysis, counterintelligence investigations, and international terrorism investigations of suspected espionage actors and known or suspected terrorists (KSTs) entering or departing the United States who may pose a threat to U.S. and DoD interests. ADIS also helps when conducting name checks on a variety of people affecting the various military branches. Such people include foreign students who have interaction with cleared defense contractors or universities conducting research. Additionally, they conduct name checks on foreigners who attend military events, such as community relations events, airshows, and military expositions.

Applicable ADIS SORN (2015) Routine Uses G, H, K.

Memorandum of Agreement between DHS and NCTC regarding ADIS Data signed (November 25, 2013).[56]

The Social Security Administration (SSA): The SSA provides social security retirement benefits and insurance benefits to millions of U.S. citizens, lawful permanent residents, and other lawfully admitted non-citizens. However, eligibility to receive certain benefits is dependent on a number of factors, including lawful immigration status and physical presence within the United States.

SSA currently works with USCIS and ICE to vet SSA benefit recipients when they first apply for benefits. In addition, SSA works with ICE to identify when an individual has been deported and thus no longer qualifies for benefit payments. In between, SSA has a knowledge gap for when individuals leave the United States for periods of time that are long enough to warrant a temporary suspension of certain benefit payments. To address this gap, CBP shares ADIS data with the SSA to determine if those individuals were still in the country and still eligible for the benefits they were receiving.

Applicable ADIS SORN (2015) Routine Use L.

[56] For more information about this Memorandum of Agreement regarding information sharing between DHS and NCTC, *see* DHS/CBP/PIA-024(a) Arrival and Departure Information System - Information sharing Update (March 7, 2014), *available at* https://www.dhs.gov/privacy.

Memorandum of Agreement between DHS CBP and SSA regarding exchanging border crossing data signed May 20, 2019.

The Department of Commerce: CBP has shared travel data containing limited PII with the Department of Commerce (DOC) for several decades, from older CBP systems. ADIS is now providing this data, as most of it pertains to Form I-94, for which ADIS will be the primary provider circa 2021. This data is provided for statistical purposes, such as estimating revenue from trade and tourism and assisting with the calculation of the United States' Gross Domestic Product.

Applicable ADIS SORN (2015) Routine Use L.

Letter of Intent between DHS CBP and DOC regarding exchanging border crossing data signed April 26, 2019.

The U.S. Census Bureau: CBP will provide arrival and departure information to the U.S. Census Bureau pursuant to Executive Order No. 13880, on *Collecting Information about Citizenship Status in Connection with the Decennial Census* (July 11, 2019), 84 FR 33821 (July 16, 2019). This sharing is consistent with 5 U.S.C. 552(b)(4), which permits disclosure of CBP information to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13. DHS is conducting a DHS-wide PIA regarding DHS datasets implicated by Executive Order 13380.

The U.S. Selective Service System (SSS): CBP sends SSS a monthly Secure File Transfer Protocol (SFTP) feed of I-94 information and SSS uses this information to determine who holds a non-immigrant visa. CBP will continue sending this SFTP feed to SSS. The SFTP feed includes only I-94 arrival and departure data.

Separately, SSS will have access to the ADIS Graphical User Interface (GUI) for government call-center employees. The users will have read-only access to all ADIS records, allowing SSS to research the travel and immigration history of people who do not register and later apply for benefits. In order to determine whether someone was required to register, SSS needs to know the individual's first date of entry and then follow his immigration history to see if he ever obtained a status that required SSS registration.

A Letter of Intent (LOI) will be completed between DHS CBP and SSS regarding Sharing of Alien Arrival and Departure Data. It outlines providing non-DHS users with a system user account. CBP will also provide access to reports, whether canned or ad hoc, as necessary. The LOI will provide interim coverage while a full Memorandum of Agreement (MOA) is drafted.

The Department of Labor (DOL)-Office of Inspector General (OIG): CBP will provide DOL-OIG access to ADIS data through its front-end user interface. This will allow DOL to query the agreed upon data elements within ADIS to support its mission of conducting criminal investigations in visa fraud, racketeering, and human trafficking, as well as overseeing the H visa

(foreign temporary workers) program. DOL users will not download information out of ADIS; it will use the query-only functionality. DOL normally will not retain any ADIS information, and will instead only use ADIS to look up a person's information to verify its own independent information. When necessary, pertinent information obtained through system queries or CBP reports will be included in OIG case or project records, including the necessary tagging and marking requirements to show that information came from ADIS. DOL-OIG will follow its existing audit and investigative records schedule for records disposition.

A Letter of Intent (LOI) will be completed between DHS CBP and DOL regarding exchanging ADIS immigration status information and providing non-DHS users with a system user account or access to ADIS data extracts. The LOI will provide interim coverage while a full Memorandum of Agreement (MOA) is drafted.