Privacy Impact Assessment
for the

Arrival and Departure Information System (ADIS)

DHS/CBP/PIA-024(b)

April 28, 2017

Contact Point
Matthew B. Schneider
Entry/Exit Transformation Office
Office of Field Operations
U.S. Customs and Border Protection
(202) 325-1086

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) contains biographic information, biometric indicators, and encounter data consolidated from various systems from DHS and the Department of State (DOS). ADIS facilitates the identification and investigation of individuals who may have violated their admission status by remaining in the United States beyond their authorized terms of entry. Other uses of ADIS include assisting in visa or immigration benefits eligibility determinations, providing information in support of national security, law enforcement, immigration and border management, intelligence purposes, as well as conducting background investigations on foreign nationals entering Federal Government facilities. This Privacy Impact Assessment (PIA) builds upon existing documentation to provide a consolidated overview of the system and its functions, and discusses new data sharing arrangements with partner agencies.

Overview

ADIS was first developed in 2002 to meet the requirements of Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, which mandates the development of an automated entry and exit control system and the matching of foreign nationals' arrival and departure records.[1] ADIS consolidates entry, exit, and admission status information from several DHS components, DOS, and the Canada Border Services Agency (CBSA) in near-real time. 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 and 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

[1] Pub. L. 104-208, 110 Stat. 3009-546.

- Providing associated testing, training, management reporting, and planning and analysis tools for administrative purposes.

A number of DHS components provide data directly to ADIS through system interfaces. These systems include:

- Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT)[2]
- CBP Advance Passenger Information System (APIS)[3]
- CBP Border Crossing Information (BCI)[4]
- CBP Non-Immigrant Information System (NIIS)[5]
- CBP TECS Secondary Inspections[6]
- U.S. Citizenship and Immigration Services (USCIS) Computer Linked Application Management System 3 (CLAIMS 3)[7] and Electronic Immigration System (ELIS)[8]
- U.S. Immigration and Customs Enforcement (ICE) Student and Exchange Visitor Information System (SEVIS)[9]

Until 2013, the US-VISIT program within the DHS National Protection and Programs Directorate (NPPD) managed both ADIS and DHS's biometric IT platform, IDENT. The 2013 Consolidated and Further Continuing Appropriations Act[10] transferred responsibility for the entry/exit mission from US-VISIT to CBP. This transfer created the Entry/Exit Transformation

[2] *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).
[3] *See* 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).
[4] DHS/CBP-007 Border Crossing Information, 81 FR 89957 (December 13, 2016).
[5] DHS/CBP-016 Non-Immigrant Information System, 80 FR 13398 (March 13, 2015).
[6] *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).
[7] *See* DHS/USCIS/PIA-016 Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems, *available at* https://www.dhs.gov/privacy.
[8] 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).
[9] *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).
[10] Pub. L. 113-6.

Office within CBP's Office of Field Operations. With the 2014 Consolidated Appropriations Act,[11] Congress directed DHS to move ADIS to CBP to align the entry/exit database with the entry/exit mission office.

Overstays, Matching Algorithms, and Data Tagging

ADIS enables CBP to better track overstays by compiling information from a variety of source systems to create a complete profile of an individual and his or her travel history. In order to determine whether an individual has violated the terms of admission into the United States and can be confirmed as an overstay, the following data points are required: the date he or she entered the United States; his or her class of admission; updates or changes to his or her visa status; and, when available, the date he or she departed the United States. CBP and other DHS components manage a variety of systems that house this information; whereas normally CBP would need to manually research and combine these elements to assess an individual's status, ADIS automates this work by bringing together the data from the variety of source systems.

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

Once ADIS creates a person-centric record based on data from the source systems, it tags the record for inclusion in one of four populations: U.S. persons (lawful permanent residents), non-U.S. persons, Special Protected Classes,[12] and potential or unconfirmed U.S. citizens. 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 and deletion if applicable, and known U.S. citizen data is filtered out prior to ingest into ADIS. USCIS provides a list of individuals associated with Special Protected Classes; these populations are tagged if the information provided matches to an ADIS record.

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,[13] E-Verify,[14] and the Systematic Alien Verification for Entitlements program[15])

[11] Pub. L. 113-76.
[12] Individuals categorized as Special Protected Classes in ADIS are those who have applied for or been granted admission into the United States under a T Visa (victim of trafficking), U Visa (victim of serious criminal activity), or the provisions of the Violence Against Women Act. Per 8 U.S.C. § 1367, information related to these individuals is subject to additional protection and may not be disclosed absent a law enforcement or national security purpose.
[13] *See* DHS/USCIS/PIA-010 USCIS Person Centric Query Service, *available at* https://www.dhs.gov/privacy.
[14] See DHS/USCIS/PIA-030 E-Verify, *available at* https://www.dhs.gov/privacy, and DHS/USCIS-011 E-Verify Program, 79 FR 46852 (August 11, 2014).
[15] *See* DHS/USCIS/PIA-006 Systematic Alien Verification for Entitlements (SAVE) Program, *available at*

- I-94 travel and departure closure messages to TECS to update traveler records; ADIS information will also be used for future I-94 public website updates to allow travelers to view their status of admission and whether they have overstayed
- Unvetted overstays and ICE Counter Terrorism and Criminal Exploitation Unit (CTCEU) leads to CBP's Automated Targeting System (ATS)[16]
- 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)[17]

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 mission needs consistent with the DHS mission. These external partners include the DOS Consular Affairs, the FBI, and the Intelligence Community.[18] In addition, CBP is exploring sharing information with other federal agencies for other purposes (for example, to determine whether benefit recipients meet time-in-country requirements). CBP will publish an update to this PIA or its appendix for any future sharing.

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, system-to-system interfaces, or data extracts.

---

https://www.dhs.gov/privacy, and DHS/USCIS-004 Systematic Alien Verification for Entitlements Program, 81 FR 78619 (November 8, 2016).

[16] *See* DHS/CBP/PIA-006 Automated Targeting System (ATS), *available at* https://www.dhs.gov/privacy, DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).

[17] *See* Privacy Impact Assessment, Consular Consolidated Database (July 17, 2015), *available at* https://foia.state.gov/_docs/pia/consularconsolidateddatabase_ccd.pdf.

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

- **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., 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.

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,[19] 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,[20] including:
  - Powers and duties of the Secretary of Homeland Security;
  - Travel and control of aliens;
  - Integrated entry and exit data system;
  - Exchange students;
  - Obligation to respond to queries from federal, state, and local government agencies on citizenship or immigration status;
  - 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.

[19] 6 U.S.C. §§ 112(b) and 202.
[20] 8 U.S.C. §§ 1103, 1185, 1201, 1225, 1365a, 1372, 1373, 1379, 1721, 1722, and 1731.

- Title 42 of the United States Code, The Public Health and Welfare (Reporting information to the Social Security Administration); [21]
- 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); and
- Homeland Security Presidential Directive 11, Comprehensive Terrorist-Related Screening Procedures (August 27, 2004).

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 for certain 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 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.[22]

[21] 42 U.S.C. § 1383(f).
[22] 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

- *DHS/CBP-021 Arrival and Departure Information System (ADIS):*[23] 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/NPPD-004 DHS Automated Biometric Identification System (IDENT):* This system is DHS's primary repository of biometric information held in support of a number of missions, including law enforcement, national security, and intelligence activities. While IDENT supplies transactional identifiers used by ADIS, the source systems for biometric collections still govern the use of the biometrics.
- *DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records:*[24] 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 December 11, 2014. 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 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?

ADIS consolidates data from a variety of systems to create a person-centric record with complete travel history information. 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.

(September 2, 2016).
[23] DHS/CBP-021 Arrival and Departure Information System, 80 FR 72081 (November 18, 2015).
[24] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (November 21, 2013).

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
- OMB 1651-0103 – Passenger List/Crew List
- 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

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

The types of information stored in ADIS include biographic data and biometric indicator information, such as:

Biographic Data:

- Full name
- Date of birth
- Social Security number (SSN)[25]
- Citizenship

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

- Nationality
- Gender
- Class of admission
- Country of residence
- Country of birth
- Travel document information (type, number, country, and date of issuance)
- Driver's license number
- Vehicle identification number
- License plate number
- 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
- Vessel port and name
- Passenger Name Record (PNR) locator number
- Arrival and departure information
- U.S. destination address
- Passenger status[26]
- Admit until date
- Passport and/or visa information and inspector comments

Biometric Indicator Data:[27]

- Fingerprint Identification Number (FIN)[28]
- Encounter Identification Number (EID)[29]

[26] A passenger's mode of transportation including, but not limited to: pedestrian, crew, vehicle, on board the vessel, and not on board the vessel.
[27] The biometric indicator data fields are associated with biometric captures in the IDENT system to provide a unique identifier.
[28] ADIS does not contain fingerprint images. Fingerprint images are assigned an identifier, which is housed in ADIS; the images themselves reside in IDENT.
[29] 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.

Vetting Data:

CBP Automated Targeting System – Passenger Module (ATS-P): As a part of the Enhanced Overstay Validation and Biographic Exit effort, CBP uses ATS-P 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 ATS-P and enriched with border crossing information,[30] SEVIS immigration and benefit information, and I-94 information.[31] ATS-P 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 would usually come 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 send biographic and biometric information to ADIS on a near-real time basis. Source system data is supplied by DHS components 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.

OBIM IDENT

IDENT may provide ADIS with the following data elements related to an individual: the Fingerprint Identification Number (FIN), Encounter Identification Number (EID), 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 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.

[30] 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).
[31] I-94 information housed within TECS is covered by DHS/CBP-016 Non-Immigrant Information System, 80 FR 13398 (March 13, 2015).

The data may be collected by IDENT data providers through an online application, a paper-based application, a mobile biometric device, a fixed platform, or in-person interviews. Latent prints may be manually collected at a 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 that 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 does not store derogatory information; rather, it uses the enforcement apprehension event type to determine whether a removal or law enforcement custody action has taken place, thus possibly closing out an overstay record in ADIS.

CBP TECS

Information that TECS[32] 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 Canadian systems. Specifically, TECS provides:

- **APIS:** CBP provides information to ADIS that was initially collected from air, sea, rail, and bus carriers or private aircraft owners about passengers and crewmembers who travel to, from, or through the United States by air, sea, rail, and bus. This information is collected 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.
- **BCI:** CBP sends to ADIS border crossing records collected 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.
    - CBSA implied exit records[33] – As part of the Beyond the Border Entry/Exit Program,[34] 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

[32] 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.
[33] 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.
[34] *See* DHS/CBP/PIA-004(h) Beyond the Border Entry/Exit Program Phase III (August 12, 2016), *available at* https://www.dhs.gov/privacy.

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),[35] 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 event in ADIS.
- **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 CLAIMS 3/ELIS

CLAIMS 3 stores information that USCIS collects from immigration benefits applications; in the future, ELIS will replace CLAIMS 3 and provide benefit information directly to ADIS.

ICE SEVIS

In addition to ADIS receiving SEVIS information through ATS-P, SEVIS also sends benefit and immigration information directly to ADIS via an automated interface.

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.

CBP 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 CTCEU and ADIS analysts review the data from separate sources and compare it to the aggregated data within

[35] *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).

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 built 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: ADIS may inadvertently receive and store data on U.S. citizens (USC) because data is transmitted from source systems that collect data from USCs.

Mitigation: This risk is partially mitigated. CBP has filters in place to prevent known USC information that is collected by source systems from being ingested into ADIS. Known USCs are identified by the presence of a U.S. passport or naturalization certificate in their travel records and are filtered out prior to ingest. In addition, ADIS has additional filters to ensure that USC information inadvertently ingested into ADIS is removed. CBP continually monitors ADIS for USCs. If found, CBP manually deletes ADIS records for any individual who is determined to be a USC, either through an encounter with CBP or for other reasons. However, if a USC presents any approved travel document (e.g., trusted traveler credential, pilot's license, military identification) other than a U.S. passport or naturalization certificate and those documents are sent to and stored in ADIS, then ADIS may not flag that individual as a USC. As a result, records of USCs may not always be removed from the ADIS production database. For example, USCs who belong to trusted traveler programs and who use the trusted traveler credential to enter or depart the United States may have information transmitted to and stored in ADIS.

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

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

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. ADIS is used by CBP, DHS components, and other federal agencies to:

- Facilitate identification and investigations of individuals who may have violated immigration statute and regulations, including their terms of admission into the United States;
- Determine 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;
- Conduct background checks on foreign nationals entering federal facilities;
- Identify instances of benefit fraud;
- Generate statistical reports on travel to and from the United States, as well as reporting on overstay rates by country; and
- Provide associated testing, training, management reporting, planning, and analysis, and for other administrative purposes.

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 use technology to 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?

As described in the ADIS data users section of this PIA, CBP, USCIS, ICE, TSA, and OCSO have read-only access to ADIS. Certain CBP employees have access rights to correct and update the ADIS data. Data from ADIS may be disclosed to users through the means described in the overview section above.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: Because ADIS is accessed by a large number of users in support of a variety of 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. ADIS information that is shared outside of DHS is shared pursuant to the routine uses listed in the ADIS SORN,[36] which serve to place limitations on the sharing of data and provide notice to the public of these uses.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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 additional notice to the public that the information they provide may be shared with other federal agencies or systems, such as ADIS. When applicable, Privacy Act

[36] DHS/CBP-021 Arrival and Departure Information System, 80 FR 72081 (November 18, 2015).

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,[37] 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.[38] Additionally, the certified school or designated 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[39] 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 a foreign national, or his or her representative, who requests to visit DHS facilities. OCSO provides the foreign national notice in written or verbal form at the time PII is collected. The foreign national 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

[37] Notice is also provided on the ESTA website, *available at* https://esta.cbp.dhs.gov/esta/application.html?execution=e1s1.
[38] *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).
[39] *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).

foreign national or the foreign national'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.[40]

DOS: The Department of State has published a PIA for the Consular Consolidated Database (CCD) and a Visa Records SORN,[41] 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 (including access to government facilities). 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.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that individuals may not be aware of 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[42] that certain information from APIS is shared with ADIS.

---

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

[41] *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).

[42] *See* DHS/CBP/PIA-001 Advance Passenger Information System (APIS), *available at* https://www.dhs.gov/privacy.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

DHS is proposing a retention schedule of 75 years, consistent with the retention schedules for ADIS source systems. 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 may inadvertently store U.S. citizen data in ADIS, thereby retaining it for longer than necessary and increasing the risk of unauthorized access, use, and loss of the data.

Mitigation: Retention of border crossing data for USCs is limited to 15 years, pursuant to the Border Crossing Information SORN.[43] 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 manually deleted. CBP continuously updates and tests ADIS tagging functionality to improve its filtering capabilities and reduce the risk of unnecessary retention of records.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government and private sector entities.

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.

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

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

As outlined in the ADIS SORN,[44] CBP uses the system in order to provide a repository of data held by DHS for 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. There are several routine uses that allow for the sharing of this information with other agencies consistent with this purpose, as described in this PIA:

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

[44] DHS/CBP-021 Arrival and Departure Information System, 80 FR 72081 (November 18, 2015).

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.[45]

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: ADIS has several attributes that help to mitigate this risk. 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. Source system data is refreshed in near real-time, with one exception of a daily refresh from USCIS 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

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

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 record is created in ADIS based on records from the source system, the record is tagged for inclusion in one of four populations: U.S. persons (lawful permanent residents), non-U.S. persons, Special Protected Classes, and potential or unconfirmed U.S. citizens. 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 and deletion if applicable; known U.S. citizen data is filtered out prior to ingest into ADIS. 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

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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 will most likely 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.[46]

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

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

1300 Pennsylvania Avenue, NW, Room 3.3D
Washington, DC 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. Through DHS TRIP, a traveler can request correction of erroneous data stored in DHS databases through one application. DHS TRIP redress requests can be made online 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, ADIS SORN, and on the DHS and CBP public facing 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, the ADIS SORN, and the source system SORNs 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 their PII regardless of his or her nationality or country of residence.

In addition, if an individual is dissatisfied with the response to his or her redress inquiry, then he or she can appeal to the DHS Chief Privacy Officer, who reviews the appeal and provides final adjudication concerning the matter. The DHS Chief Privacy Officer can be contacted at:

Chief Privacy Officer, Attn: DHS Privacy Office
Department of Homeland Security, Mailstop 0655
245 Murray Drive, SW
Washington, DC 20528
Fax Number: (202) 343-4010

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 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

The following questions are intended to describe technical and policy based safeguards and security measures.

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, CBP employees must have undergone a Tier 4 or a Tier 5 (Single Scope) Background Investigation, and be favorably adjudicated to hold a high risk or critical sensitive position. All investigations must be in-scope (less than five years old) 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. All users are required to read and sign a Rules of Behavior form before accessing ADIS.

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

Matthew B. Schneider, Assistant Director
Entry/Exit Transformation Office
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, sign copy on file at 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 determine if an individual previously overstayed his or her terms of admittance and to 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 Automated Targeting System Person (ATS-P), which enables automated and manual queries to support vetting and targeting operations. CBP Office of Field Operations ADIS Vetting Unit (AVU) analysts use ADIS user accounts to help determine the status of lawfully admitted aliens that depart beyond their period of authorized stay (or "overstays"). CBP analysts consolidate travel and immigration history from different sources and create a complete travel and immigration history of an individual.

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 DHS components can access ADIS data through PCQS.

ICE Homeland Security Investigations (HSI) Counterterrorism and Criminal Exploitation Unit (CTCEU): CTCEU analysts use ADIS user accounts to help determine the status of lawfully admitted aliens that remain in the United States beyond their period of authorized stay (or "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 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).

OCSO: OCSO uses ADIS user accounts to assist in confirming the identity of foreign nationals 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 foreign national identity verification. OCSO then notifies the submitting components of the vetting process results.

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.

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.

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.

Appendix B

Authorized ADIS Users Outside of DHS

The U.S. Department of State, Bureau of Consular Affairs (CA): CA 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. CA also uses aggregated ADIS data to identify overstay trends for various visa categories and visa issuing posts. ADIS has been supporting CA since 2003.

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, Foreign Terrorist Tracking Task Force (FTTTF): ADIS provides information to the FTTTF to assist in mitigating potential national security risks and threats. 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.

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,[47] 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 information technology security is in place during and after ADIS data is sent, 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.

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

Memorandum of Agreement between DHS and NCTC regarding ADIS Data signed (November 25, 2013).[48]

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

[47] Pub. L. 108-458 (December 17, 2004).
[48] For more information about this Memorandum of Agreement regarding information sharing between DHS and NCTC, please *see* DHS/CBP/PIA-024(a) Arrival and Departure Information System - Information sharing Update (March 7, 2014), *available at* https://www.dhs.gov/privacy.

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 piloted an initial data exchange with the SSA in 2016. CBP queried approximately 11,000 SSA records against ADIS to determine if those individuals were still in the country and still eligible for the benefits they were receiving. As this was a test of the data exchange and analysis, the results were used only for informing the test and were not used operationally to deny certain benefit payments to individuals.

Pending ongoing analysis of the results, CBP will work with SSA to develop a fully operation capability in Fiscal Year 2017-2018.

Applicable ADIS SORN (2015) Routine Use L.

Letter of Intent between DHS CBP and SSA regarding exchanging traveler border crossing data signed April 4, 2016.