Privacy Impact Assessment
for the

Central Index System (CIS)

DHS/USCIS/PIA-009(a)

April 7, 2017

Contact Point
Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
(202) 272-8030

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. Citizenship and Immigration Services (USCIS) maintains the Central Index System (CIS). CIS contains information on the status of applicants and petitioners seeking immigrant and non-immigrant benefits to include: lawful permanent residents, naturalized citizens, United States border crossers, aliens who illegally entered the United States, aliens who have been issued employment authorization documents, individuals who petitioned for benefits on behalf of family members, and other individuals subject to the provisions of the Immigration and Nationality Act (INA). USCIS is updating and reissuing the CIS Privacy Impact Assessment (PIA) to clarify CIS' functionalities and to update the systems interconnected to CIS.

Overview

U.S. Citizenship and Immigration Services (USCIS) oversees lawful immigration to the United States and is responsible for processing petitions, applications, and other requests for immigration benefits. The Central Index System (CIS) was originally established to support the legacy Immigration and Naturalization Services (INS) records management needs to collect and disseminate automated biographic and historical information related to individuals during the immigration life cycle. CIS is now being fully used by Department of Homeland Security (DHS) components and is maintained by USCIS.

CIS serves as a DHS-wide index used to track the location of case files, to include Alien Files (A-File)[1] nationally and to maintain alien status and repository information. CIS contains information on the status of individuals, including lawful permanent residents, naturalized citizens, U.S. border crossers, apprehended aliens, legalized aliens, aliens who have been issued employment authorizations, and other individuals of interest to DHS. CIS provides information used for granting or denying benefits and capturing subsequent status changes; documenting chain of custody for enforcement; keeping track of immigrant statistics; and control and account of record keeping services in accordance with the Code of Federal Regulations (CFR) to certify the existence or non-existence of records.

CIS is a repository of electronic data that summarizes the history of an immigrant in the adjudication process. In addition, CIS maintains the same information about individuals of interest

[1] A-File, a paper or electronic-based file that contains official immigration records of aliens or persons who are not citizens or nationals of the United States, as well as U.S. born citizens involved in certain immigration crimes. A-Files contain all records pertaining to naturalized citizens and any active case of an alien not yet naturalized, including records created as he or she passes through the U.S. immigration and inspection process and, when applicable, records related to any law enforcement action against or involving the alien.

to the U.S. Government for investigative purposes. Information contained within CIS is used for immigration benefit determination and for immigration law enforcement operations by USCIS, U.S. Immigration and Customs Enforcement (ICE), and U.S. Customs and Border Protection (CBP). Information contained within CIS is also used by federal, state, and local benefit programs, and by federal, state, and local law enforcement entities.

Record Creation

DHS assigns an individual a unique identification number that is known as an Alien Number (A-Number)[2] when the individual applies for immigration-related benefits, or is the subject of a law enforcement action.[3] A-Numbers may also be issued by the Department of State (DOS) in limited circumstances overseas for the issuance of visas. In order to collect and maintain hard copy information relating to individuals who have been issued A-Numbers, DHS creates an A-File, which may include both paper-based and electronic files. An A-File is the series of records that USCIS maintains on individuals under the purview of the INA and relevant regulations, which documents the history of their interaction with DHS as required by law. USCIS is the designated custodian of A-Files for all of DHS.

After a paper A-File is generated for a person, USCIS Records Personnel electronically create a record in CIS capturing eight mandatory data fields from the benefits application, visa application, or law enforcement document. These mandatory data elements include the Alien Number, first name, last name, date of birth, File Control Office (FCO), country of birth, date of file opened, and class of admission. CIS may contain additional information from documents provided by the applicant when applying for benefits or visas or from information provided by law enforcement officials due to an encounter.

Only Records personnel and/or Records contract staff are designated and trained to perform the electronic creation of an entry in CIS. The A-File may include information on U.S. citizens if the individual's immigration status is derived or acquired based on his or her relationship to a U.S. citizen as well as if the individual has successfully completed the immigration process and been naturalized.

[2] The A-Number is a unique seven-, eight- or nine-digit number assigned to a noncitizen at the time his or her A-File is created.

[3] As a general matter, USCIS does not create an A-Number on a native born U.S Citizen. However, in the event that a person (native born or naturalized) decides that he or she does not want to be a U.S. citizen, he or she may formally renounce his or her citizenship through Department of State (DOS). DOS sends a Certificate of Loss of Nationality to USCIS to be filed in an A-File for this purpose. In such circumstance an A-File will be created. A-Files are not created on U.S. born citizens that violate an immigration law.

Record Updates

CIS is a repository of electronic data that summarizes the history of an immigrant in the adjudication process. In addition, CIS maintains the same information about individuals of interest to the U.S. Government for investigative purposes related to the immigration process. CIS serves as the focal point for many disparate USCIS systems to consolidate information about a person requesting benefits. In the current USCIS environment, there are multiple benefits processing systems and support systems. CIS sends and receives updates from these systems to keep the most up-to-date record of an A-File's (Applicant's benefit request virtual and physical file folder) status and location.

CIS collects data from other systems to receive and shares timely and accurate information. CIS interfaces with the following USCIS, DHS, and external systems, on a nightly basis, to either consolidate or share the latest status of an individual's case.

USCIS Systems

- **Electronic Document Management System** (EDMS) notifies CIS when an A-File is digitized so CIS can display the digitized banner. CIS sends EDMS metadata for records that are digitized to be added to EDMS.[4]
- **USCIS Electronic Information System (USCIS ELIS)** is an electronic case management system that allows USCIS to process certain immigration benefit requests. ELIS sends visa packet data for lawful permanent residents, and I-551 card, Employment Authorization Document, and naturalization data for adjudicated applications that modifies personnel data, and adds card and history transactions to CIS.[5]
- **Computer-Linked Application Information Management System 3** (CLAIMS 3) provides data on application/petition receipting, fingerprint checks, and adjudication while receiving personal data changes, history transactions, and error files.[6]
- **Computer-Linked Application Information Management System 4** (CLAIMS 4) provides automated support for the processing of Application for Naturalization (N-400) forms, including the receiving, data entry, and other initial processing operations of the USCIS Service Centers, as well as the adjudications and oath ceremony management activities of the local USCIS offices. CLAIMS 4 sends three different application data: Central Index Close, File Transfer Request, and Verify Data.[7] CIS sends special protected

[4] *See* DHS/USCIS/PIA-003 Integrated Digitization Document Management Program (IDDMP) *available at* www.dhs.gov/privacy.
[5] *See* DHS-USCIS-PIA-056 USCIS ELIS *available at* www.dhs.gov/privacy.
[6] *See* DHS/USCIS/PIA-016(a) Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems *available at* www.dhs.gov/privacy.
[7] *See* DHS/USCIS/PIA-015 Computer Linked Application Information Management System (CLAIMS 4) Update

class data to CLAIMS 4 on a daily basis.[8]

- **Marriage Fraud Act Amendment System** (MFAS) provides history transaction and visa packet data and receives personnel data changes, history transactions, and error files.[9]
- **National File Tracking System** (NFTS) sends file transfer data and receives confirmation and error files.[10]
- **Refugee Asylum and Parole System** (RAPS) provides the means for automated tracking of asylum cases as they progress from application filing through final decision of grant, denial, or referral to the U.S. Immigration Courts. RAPS sends asylum case status data to CIS. CIS sends special protected class data to RAPS on a daily basis.[11]
- **Verification Information System** (VIS) supports the functionality for performing alien status inquiries by government agencies and employers by performing the initial verification (primary query request), additional verification (secondary query request), and DHS referrals. VIS receives alien verification information from CIS daily.[12]

Other DHS Systems

- **U.S. Customs and Border Protection (CBP) Advance Passenger Information System (APIS)** supports the review of passenger information prior to boarding for commercial flights arriving into or departing from the United States and for commercial vessels destined for or departing the United States. CIS sends special protected class data to APIS on a daily basis.[13]
- **CBP Arrival Departure Information System (ADIS)** is a system that aggregates certain records from a number of border crossing and immigration systems. It was created to identify individuals who were lawfully admitted to the United States but subsequently overstayed their permission to remain. This is accomplished by tracking entry and exit encounters during a variety of DHS's interactions with the public, such as the immigrant

available at www.dhs.gov/privacy.

[8] Special protected classes of individuals include nonimmigrant status for victims of human trafficking, nonimmigrant status for victims of crimes, and relief for domestic violence victims.

[9] MFAS is a subsystem of CLAIMS 3 MF. *See* DHS/USCIS/PIA-016 Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3) *available at* www.dhs.gov/privacy.

[10] *See* DHS/USCIS/PIA-032 National File Tracking System (NFTS) *available at* www.dhs.gov/privacy.

[11] *See* DHS/USCIS/PIA-027 Refugees, Asylum, and Parole System (RAPS) and the Asylum Pre-Screening System (APSS) *available at* www.dhs.gov/privacy.

[12] VIS is the technical infrastructure that enables USCIS to operate Systematic Alien Verification for Entitlements (SAVE) and E-Verify. For more information on these programs, *see* DHS/USCIS/PIA-006 Systematic Alien Verification for Entitlements (SAVE) Program and its updates and DHS/USCIS/PIA-030 E-Verify Program and its updates *available at* www.dhs.gov/privacy.

[13] *See* DHS/CBP/PIA-001(g) - Advance Passenger Information System (APIS) and its updates *available at* www.dhs.gov/privacy.

and non-immigrant pre-entry, entry, and exit processes. CIS sends special protected class data to ADIS on a daily basis.

- **CBP Automated Targeting System (ATS)** is a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based scenarios and assessments. CIS sends special protected class data to ATS on a daily basis.[14]
- **CBP Data Sharing Initiative (DSI)**, sends immigrant visa applicant data (*i.e.*, Alien Number, name, and date of birth) to CIS.
- **CBP Electronic System for Travel Authorization (ESTA)** is a web-based application and screening system used to determine whether citizens and nationals from countries participating in the Visa Waiver Program are eligible to travel to the United States. CIS sends special protected class data to ESTA on a daily basis. CIS sends special protected class data to ESTA on a daily basis.
- **CBP TECS** provides controlled access to a large database of law enforcement information that interfaces with other federal, state, and international law enforcement systems. TECS major functions support passenger processing and investigations. TECS sends Alien Number, Date of Birth, and National Automated Information Lockout List flag to CIS.[15] CIS sends special protected class data to TECS on a daily basis
- **U.S. Immigration and Customs Enforcement (ICE) Enforcement Alien Removal Module (EARM),** is t case management system related to Detention and Removal Operations for alien removals. EARM provides enhancements such as biometric identification, electronic forms, operational reports, photographs, and interfaces to other alien-centric data stores. EARM provides deportation information to CIS on a nightly basis and may be viewed from CIS the next business day.[16]
- **ICE Student and Exchange Visitor Information System (SEVIS)** maintains real-time information on nonimmigrant students and exchange visitors, their dependents, and the approved schools and designated U.S. sponsors that host these nonimmigrants. CIS sends special protected class data to SEVIS on a daily basis.[17]
- **DHS Data Framework** creates a systematic repeatable process for providing controlled

[14] *See* DHS/CBP/PIA-006(e) Automated Targeting System *available at* www.dhs.gov/privacy.
[15] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS) and its updates *available at* www.dhs.gov/privacy.
[16] *See* DHS/ICE/PIA-015 Enforcement Integrated Database and its updates *available at* www.dhs.gov/privacy.
[17] *See* DHS/ICE/PIA 001 Student Exchange Visitor Information System (SEVIS) *available at* www.dhs.gov/privacy.

access to DHS data across the Department. Currently the DHS Data Framework includes the Neptune and Cerberus systems, and the Common Entity Index. CIS sends special protected class data to the DHS Data Framework on a daily basis.[18]

External Systems

- **Department of State Consular Lookout and Support System (CLASS)** is used to perform name checks of visa and passport applicants in support of issuance processing and document verification. CIS sends special protected class data to CLASS on a daily basis.[19]
- **Social Security Number Establishment and Correction System (SSNEC)**, **Social Security Administration (SSA)**, assigns new Social Security numbers (SSN) and issues original and replacement Social Security cards. SSNEC contains all of the information received on original applications for SSNs and applications supported by evidence suspected or determined to be fraudulent. CIS sends enumeration file information (*i.e.*, SSN, name, A-Number) to SSNECS.[20]
- **Large Business and International (LB&I)/International Individual Compliance (IIC)**, **Internal Revenue Service (IRS)**, CIS provides Abandonment of Citizenship information to IRS LB&I/IIC on a quarterly basis.[21] The file USCIS MF/CIS sends contains specific information related to the abandonment of his or her U.S. citizenship. No data is sent to CIS from LB&I/IIC. This is a one-way interconnection.[22]

System Auditing

Transaction Record Keeping System (TRKS), a subsystem of CIS, captures any modifications made to a record associated by an A-Number by a system user or system update. The primary purpose of TRKS is to provide an audit trail of the activities performed by CIS users. The audit trail includes any additions, deletions, or modifications, along with recording the viewing of selected information. The audit information is used to detect and investigate misuse of CIS. The system also assists in capturing and reporting statistical information on CIS use.

Account Searches

CIS is a searchable application. The information stored in CIS may also be accessed by USCIS and other DHS agencies (*i.e.*, CBP, ICE). CIS allows DHS field offices, ports of entry, and examination and inspection sites prompt access for accurate biographical and status information

[18] *See* DHS/ALL/PIA-046(a) DHS Data Framework available at www.dhs.gov/privacy.
[19] *See* Consular Lookout and Support System (CLASS) PIA *available at https://2001-2009.state.gov/documents/organization/96128.pdf*.
[20] *See* 016-00-SSA/DCS-M-003 Social Security Number Establishment and Correction System PIA *available at* www.socialsecurity.gov/foia.
[21] Internal Revenue Code (IRC) Section 6039G(d)(3)
[22] *See* LB&I Data Capture System PIA *available at* https://www.irs.gov/pub/irs-utl/dcs-2-pia.pdf.

on individuals seeking legal entry to or residence in the United States, thus ensuring proper entry and granting of benefits to eligible individuals. CIS also assists DHS in the identification of individuals who violate the terms of their stay. Additionally, CIS allows DHS field offices to identify the location and timely access to hard copy A-Files on individuals of interest to DHS. USCIS and other DHS users may access CIS directly or through the Person Centric Query System (PCQS).[23] Both interfaces provide read-only access to CIS.

USCIS enhanced CIS to tag records relating to a protected individual and to provide those accessing the information with notice of specific procedures regarding the disclosure and use that apply to the protected information. For instance, CIS includes an alert message to indicate that an individual is protected by 8 U.S.C. § 1367. The message reads: *8 USC 1367 Protected Information–Disclosure and Use Restrictions Apply*. The statutory confidentiality protections at 8 U.S.C. § 1367 generally prohibit the disclosure or use of any information about applicants for, and beneficiaries of, certain victim-based immigration benefits, including T nonimmigrant status, U nonimmigrant status, or relief under the Violence Against Women Act (VAWA). Applicants for, and beneficiaries of, these benefits are those people who have been victimized by others, including human traffickers, criminal gangs, or abusive spouses or partners. Beneficiaries may also include qualifying family members (derivatives) of the victim. The law requires that this information about principal applicants and their derivatives must be protected from disclosure in order to avoid endangering the victims by providing their victimizers any personal information about them. These confidentiality protections generally continue indefinitely; they may terminate only when the application for relief is denied and all opportunities for appeal of the denial have been exhausted. Any record in CIS that displays this banner must be handled as Section 1367 Information in accordance with USCIS policy.

Historic Files

USCIS maintains A-File information captured prior to 1940 in historical files that are contained on microfiche, microfilm, index cards, and in certificate files. These historic records have moved into the Microfilm Index Digitization Application System (MiDAS)[24], designed to capture the information from these older decaying types of media. Only the information contained in naturalization certificate files contains the eight data elements required by CIS to allow it to be created electronically in the system so the file may be sent to another location for review if requested. This is the only time that information contained in MiDAS will also be in CIS.

[23] *See* DHS/USCIS/PIA-010 Person Centric Query Service (PCQS), *available at* www.dhs.gov/privacy.
[24] *See* DHS/USCIS/PIA-017 Microfilm Digitization Application System (MiDAS), *available at* www.dhs.gov/privacy.

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 authority to collect information in the CIS is set forth in the Immigration and Nationality Act, 8 USC §§ 1101, 1103, 1304 et seq., and implementing regulations found in 8 CFR.

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

The Alien File, Index, and National File Tracking System of Records covers the collection, use, and maintenance for information in CIS.[25]

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

Yes. CIS is covered as a subsystem under the USCIS Mainframe Applications accreditation boundary. The USCIS MF Security Plan was completed on April 15, 2014. The USCIS MF Authority to Operate was granted on September 2, 2014 and will expire on September 1, 2017. The USCIS Mainframe Applications is planned to move to Ongoing Authorization status, which provides continuous monitoring and no specific expiration date.

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

Yes. NARA approved the CIS retention schedule [N1-566-10-01] on November 05, 2009. CIS records are permanent and USCIS transfers A-Files to the custody of NARA 100 years after the individual's date of birth.

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.

Not applicable. CIS is not subject to the Paperwork Reduction Act requirements.

[25] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (Nov. 21, 2013).

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.

CIS contains information on those individuals who during their interactions with DHS or DOS have been assigned an A-Number. The system contains biographic information on those individuals allowing DHS employees to quickly review the individual's immigration status. The information in CIS may also be used to request the hard copy A-File from the DHS File Control Office that has custody of the file. Specific data elements maintained in CIS may include:

- Full Name;
- Alias(es);
- Gender;
- Date of Birth;
- Country of Birth;
- Country of Citizenship;
- Port of Entry;
- Date of Entry;
- Class of Admission;
- A-Number;
- Social Security number (or other number originated by a government that specifically identifies an individual);
- I-94 Admission Number;
- Passport Number;
- Federal Bureau of Investigation (FBI) Identification Number;
- Legacy INS Fingerprint Number;
- DHS Automated Biometric Identification System (IDENT) Fingerprint Identification Number;[26]

[26] *See* DHS/NPPD/USVISIT/PIA-002 Automated Biometric Identification System (IDENT), *available at*

- Driver's License Number;
- Derivative Citizenship Certificate Number (DA, AA, AB, and EE Numbers);[27]
- Naturalization Certificate Number (C-Number);
- Naturalization Date;
- Naturalization Court;
- Naturalization Location;
- Mother's Name;
- Father's Name;
- File Control Office (FCO);
- File Information (*i.e.*, file transfer request, initiation, and confirmation date); and
- Deportation Information, such as: biometric identification, electronic forms, operational reports, fingerprint ID numbers, and interfaces to other alien-centric data stores.

There are eight mandatory fields required to create a new record in CIS. The mandatory data elements include: A-Number, first name, last name, date of birth, class of admission, country of birth, creation date of file, and the FCO (local file control offices) identifying where the file is located.

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

The majority of the information contained in CIS is obtained directly from the individual requesting immigration benefits, provided for in the INA, on behalf of him or herself or others filed either with DHS or with DOS on an OMB approved form. Other information may be derived from records resulting from enforcement operations when a person is apprehended at the border, internally in the United States, or when a person has a warrant for deportation. Information is gathered from enforcement forms within ICE and CBP, then used to create physical A-Files, and later followed by Records personnel creating a record in CIS.

Additionally, information collected from other systems is used to augment and validate the information. CIS receives data from other USCIS, DHS, and external systems to create the A-File summary and tracking information.

---

www.dhs.gov/privacy.

[27] More information on Certificate Series Numbers is available at https://www.uscis.gov/history-and-genealogy/genealogy/certificate-series-numbers.

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

No.

2.4 Discuss how accuracy of the data is ensured.

USCIS collects information primarily from the benefit requestor or beneficiary or his or her representative. ICE and CBP also collect information during enforcement operations. USCIS, ICE, and CBP are dependent on the individual to provide accurate information.

USCIS creates a record in CIS based on the A-File. The physical creation of a new file can be prepared by several authorized individuals; however, the electronic creation and input of data can only be accomplished by USCIS Records personnel or USCIS Records contract staff who are trained and designated to perform this function. An A-File is not considered to be created until it has been electronically created within CIS. This creation requires that one individual enters the data while another individual verifies the accuracy of the information derived from the physical A-File. The verification process must be completed within 48 hours or the information will be deleted from the system. Any information uploaded from another system undergoes a series of automated data checks before being added to the system. CIS generates error reports in the event a record is rejected due to faulty, incomplete or incorrect data. The USCIS File Control Office that entered the uploaded information will be notified of the error and must address the noted deficiency prior to re-sending the information.

USCIS developed procedures for updating the information if users notice inconsistencies between the paper A-File and CIS. Only a limited number of authorized USCIS Records personnel may update the system accordingly.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the information in CIS may be inaccurate due to manual entry of data.

Mitigation: Only authorized USCIS Records staff have the ability to add or edit data and create A-Numbers electronically. CIS validates data entry through program coding to mitigate or prevent inconsistencies in applicant data and in decision processing entries (*e.g.*, the system rejects 00/00/00 birthdates). Validation checks are performed when the data is entered and verification of the data is performed by subsequent processing and cross-checked with other sources. Data entry personnel are provided with the opportunity to review and edit information prior to and after their submission.

Privacy Risk: There is a risk that USCIS, DHS, and other external users may update CIS with incorrect information.

Mitigation: USCIS partially mitigated this risk. Only a few USCIS employees are able to make edits directly in CIS. Most users of CIS only have read-only access through CIS directly or through PCQS. Those users must go to the source system to make changes to data that would reflect in CIS when the data refreshes on a nightly basis. CIS is unable to validate whether the changes made in the source system are accurate.

Privacy Risk: There is a privacy risk that an individual was issued more than one A-Number resulting in multiple records in CIS.

Mitigation: This risk is partially mitigated. The A-Number is a major key to locating data in CIS. USCIS may identify that more than one A-File was issued to an individuals. In the event that an individual was inadvertently issued more than one A-Number, USCIS lists all A-Numbers for subjects who may have had multiple A-Numbers assigned in his or her CIS record. USCIS reviews all of the multiple A-Numbers identified during the CIS check. USCIS consolidates all A-Numbers in CIS by identifying primary and secondary A-Numbers. A primary A-Number is the number currently assigned to the surviving physical paper file and it is the first number listed in CIS. A secondary A-Number(s) are those that been consolidated into the primary A-Number, and are listed below the primary number.

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.

CIS is a repository of electronic data that contains an index of basic data elements related to an individual as he or she passes through the immigration process. The purpose of CIS is to provide a searchable central index of A-Files and to support the location and transfer of A-Files among DHS personnel and offices as needed in support of immigration benefits and enforcement actions. This purpose includes the ability to ascertain an individual's current immigration status (class of admission) and prior status (class of admission).

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.

No.

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

CBP and ICE have read-only access to CIS directly and/or through PCQS. Information is accessible by all CBP and ICE personnel so that they may perform their mission requirements. CBP uses CIS for border and inspection processes. ICE uses CIS for investigatory, deportation, and immigration court functions.

External agencies (*i.e.*, DOS, Drug Enforcement Administration (DEA), International Criminal Police Organization (INTERPOL), and SSA) may access CIS directly or through PCQS). External agencies may include other federal, state, and local benefit bestowing programs, and by federal, state, and local law enforcement entities. These agencies have read-only access to the database. Some of these external users can access CIS through ICE user accounts. These users are granted read-only access using the ICE Password Issuance and Control System (PICS) process based on a background investigation and are indistinguishable from ICE employees. Information Sharing Agreements (ISA) have been created between ICE and these agencies. There are also external users who may access CIS through CBP, such as the DOS. These users are granted read-only access by CBP based on a background investigation and are indistinguishable from CBP employees.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that authorized users could use the data for purposes inconsistent with the original collection.

Mitigation: The risk is partially mitigated. To ensure the information is used consistently with the purposes of the original collection, USCIS monitors audit logs to ensure users are only accessing information related to their job functions. Prior to accessing CIS, each DHS user must sign a user access agreement that outlines the appropriate rules of behavior tailored to CIS. External agency representatives viewing the data must sign a non-disclosure agreement, which outlines the limits and restrictions regarding use of the data. Agencies requesting access to information/files are required to send a memorandum on official letterhead, signed by the local director, with an accreditation list identifying the names of those individuals that have been authorized to review information contained within USCIS records/systems.

USCIS implements disciplinary rules to ensure the appropriate use of the system. USCIS reminds employees accessing the system that the system may be monitored for improper use and illicit activity, and the penalties for non-compliance, through a warning banner that reiterates the appropriate uses of the system. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. This process acts as a deterrent to unauthorized activity.

Privacy Risk: There is a risk that unauthorized users may gain access to CIS.

Mitigation: This risk is partially mitigated. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards such as restricting access to authorized personnel who have a need-to-know. In addition to DHS users, CIS has external users that can logon and run queries through ICE credentials, such as law enforcement agencies, and Task Force Teams. These users may not be uniquely identified since the access may be provided via another agency.

CIS is an application that is only available through the DHS USCIS network. All access is secured through access controls requiring PIV card. Authorized employees must use their issued credentials, also known as PIV cards to gain access to CIS. Individuals who do not require access to CIS will not be able to access CIS through their PIV card. Access to the system via PIV card is consistent with the National Institute of Standards and Technology 800-63 Level 4-assurance of the user's identity.[28]

Privacy Risk: There is a risk that USCIS may provide unauthorized individuals access to CIS.

Mitigation: Since the formation of DHS, Read-Only access to information contained in CIS has been provided to the following three components: 1) CBP, for border and inspection process; 2) USCIS, for immigration benefit adjudication process; and 3) ICE, for investigatory, deportation, and immigration court functions. Information is accessible by all three components so that they may perform their mission requirements. Officers have read-only access, and include adjudications officers who review applications and assign benefits, and enforcement officers who encounter individuals at the ports of entry, borders, and interior of the United States, and must verify the status of those individuals. Only specific authorized USCIS Records users have the ability to add or edit data and create and verify A-Numbers electronically. USCIS is careful to only share data with other DHS components who need to know the information. Only USCIS internal users, System Administrators, and Data Base Administrators have write and modify access to the CIS application and CIS database files.

Privacy Risk: There is a risk that USCIS may inadvertently disclose special protected class

[28] *See* NIST Special Publication (SP) 800-63-2, Electronic Authentication Guideline, dated August 2013, *available at* http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf.

data (T, U, VAWA) without a need-to-know.

Mitigation: USCIS has partially mitigated this risk. CIS includes an alert message to indicate that an individual is protected by 8 U.S.C. § 1367. The release will help users comply with 8 U.S.C § 1367(a), which prohibits DHS from making unauthorized disclosures of information related to certain protected classes of aliens, including applicants and recipients of T (victims of human trafficking) and U (victims of criminal activity) visas, and relief under the Violence Against Women Act of 1994 (VAWA). This enhancement also makes CIS users immediately aware that they are displaying a record relating to a protected individual and that specific procedure regarding the disclosure and use apply. Any record in CIS that displays this banner must be handled as Section 1367 Information in accordance with USCIS policy.

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.

The instruction associated with each benefit request form contains a Privacy Act Statement. Each Privacy Act Statement provides notice to individuals about the agency's authority to collect information, the purposes of data collection, routine uses of the information, and the consequences of declining to provide the requested information to USCIS. Additionally, the forms also contain a provision by which an applicant authorizes USCIS to release any information received from the benefit requestor or beneficiary as needed to determine eligibility for benefits. Furthermore, individuals are provided general notice through the publication of this PIA and the Alien File, Index, and National File Tracking System SORN.[29]

In instances in which the A-File is created for other purposes (*e.g.*, enforcement, investigations), information may not be collected directly from the individual, and thus, the individual may not have an opportunity to decline to provide information contained within the A-File.

[29] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (Nov. 21, 2013).

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

The submission of a benefit request is voluntary. To grant the requested benefit, applicants must provide certain biographic and biometric information that may include submission of fingerprints, photographs, and signatures, in addition to other information requested in an application. This information is critical in making an informed adjudication decision to grant or deny an immigration benefit. Failure to provide the requested information prohibits USCIS from processing and properly adjudicating the application and thus precludes the applicant from receiving the benefit. For A-Files created for other purposes (*e.g.*, enforcement, investigations), the individual does not consent to particular uses of the information.

4.3 Privacy Impact Analysis: Related to Notice

USCIS provides general notice to the public through this PIA and the joint USCIS, CBP, and ICE A-File SORN. The extent of notice and opportunity to provide informed consent varies based on the particular purpose associated with the original collection of the information. In most cases, notice is provided when the applicant fills out the form or application for benefits. For the other information collected in CIS, because of the law enforcement and customs and immigration purposes for which the information is collected, opportunities for the individual to be notified prior to the collection of information may be limited or nonexistent. Individuals may be notified by other law enforcement agencies at the point of collection of the original data that their information may be shared for law enforcement purposes. Because USCIS does not directly collect most of the information gathered by ICE or CBP, USCIS is also not in the best position to provide individuals notice prior to the collection of information.

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.

Under the NARA approved the CIS retention schedule [N1-566-10-01], CIS records are permanent and USCIS transfers CIS records to the custody of NARA 100 years after the individual's date of birth. Newly-eligible files are transferred to the National Archives every five years.

5.2 Privacy Impact Analysis: Related to Retention

There is no privacy risk related to retention. NARA determined CIS records to be of permanent historical value. USCIS retains data beyond the approval or denial of a benefit in order to ensure the information is available for several purposes, including future immigration status verification, evaluating subsequent benefits sought by an applicant, and for litigation.

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.

Information in CIS is used on a daily basis by DHS operational components, as well as by various federal and state entitlement and law enforcement programs. These external agencies are provided read-only access to CIS directly or through the PCQS or through a system interconnection. Some external users can access CIS through ICE or CBP user accounts.

Department of State (DOS)

USCIS and DOS are partners in the processing of certain immigration benefit cases. DOS has read-only access to CIS directly thought CBP credentials and through PCQS. Access to CIS provides DOS with information on USCIS adjudications of benefits and other decisions relating to non-immigrant and immigrant visas, and naturalization cases. This includes data on current immigration status and historical information. This data sharing arrangement allows USCIS and DOS to increase processing efficiency and maintain a comprehensive picture of a benefit requestor's status from visa application to naturalization.

Social Security Administration (SSA)

USCIS, DOS, and the SSA currently have a Memorandum of Understanding (MOU) in place that covers the process in which USCIS issues SSNs and Social Security cards in an automated manner (*i.e.*, individual does not have to visit a Social Security Office) to immigrants through a process called Enumeration at Entry (EAE). EAE is a joint effort between DOS, USCIS, and SSA. As part of the DOS immigrant visa application process, immigrants outside the United States have the option to apply for an SSN card at the same time they apply for an immigrant visa. Once DOS approves their visa application and DHS admits them into the United States for permanent residence, SSA automatically issues the SSN card. USCIS electronically transmits to

SSA enumeration data for resident aliens with employment authorization who request a SSN or replacement Social Security card. This process will allow USCIS benefit seekers to request a SSN or replacement card as part of the USCIS benefit process.

Department of Justice (DOJ)

DHS/ICE users at FBI facilities with network and system access to CIS support the Joint Terrorism Task Force (JTTF). The JTTF is tasked with investigating, detecting, interdicting, and removing, prosecuting terrorists, and dismantles terrorist organizations.

Internal Revenue Services (IRS)

DHS is required to provide the IRS with the names of individuals who choose to abandon their LPR and citizenship status. USCIS shares CIS data with IRS through a system interconnection. This system interconnection allows CIS to provide abandonment of citizenship information to IRS on a quarterly basis, as directed by legal requirements and mandates. CIS sends specific information related to the abandonment of an individual's United States citizenship. This is a one-way interconnection; no data is sent to CIS from LB&I/IIC.

Local Law Enforcement

Local law enforcement agencies, such as police and sheriff's offices, cooperate with federal agencies in investigations of illegal activities that may involve aliens that are provided by ICE. Such investigations may require the retrieval or update of information contained in an individual's A-file. These users are granted access using the ICE PICS process based on a background investigation and are indistinguishable from ICE employees. ISAs have been created between ICE and these agencies.

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

DOS

Sharing USCIS data to DOS is compatible with the purpose of the system because the DOS mission, like USCIS, includes ensuring lawful visits and immigration to the United States as dictated by the INA. Routine Use O of the A-File SORN permits USCIS to share information with the DOS for the purpose of processing petitions or applications for benefits under the INA, and all other immigration and nationality laws including treaties and reciprocal agreements; or when the Department of State requires information to consider and/or provide an informed response to a request for information from a foreign, international, or intergovernmental agency, authority, or organization about an alien or an enforcement operation with transnational implications.

SSA

Sharing USCIS data to SSA is compatible with the purpose of the system because section 205(b)(2) of the Social Security Act, as amended, authorizes SSA to issue a Social Security card to aliens at the time of their lawful admission to the United States. Routine Use DD of the A-File SORN permits the sharing of information to SSA for the purpose of issuing a SSN and card to an alien who has made a request for a SSN as part of the immigration process and in accordance with any related agreements in effect between the SSA, DHS, and DOS entered into pursuant to 20 CFR 422.103(b)(3), 422.103(c)(3), and 422.106(a), or other relevant laws and regulations.

DOJ

Sharing USCIS data with DOJ is compatible with the purpose of the system because the DOJ mission, like USCIS, includes ensuring lawful visits and immigration to the United States as dictated by the INA. Routine Use N of the A-File SORN permits USCIS to share with DOJ (including Offices of the United States Attorneys) or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when necessary to assist in the development of such agency's legal and/or policy position.

Routine Use G of the A-File SORN permits USCIS to share information with DOJ when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

IRS

Sharing USCIS data with IRS is compatible with the purpose of the system because USCIS is required by law to provide the IRS with the names of individuals who choose to abandon their lawful permanent resident (LPR) status. Routine Use CC of the A-File SORN permits USCIS to share information with IRS to verify or ascertain the citizenship or immigration status of any individual within the jurisdiction of the agency for any purpose authorized by law.

Local Law Enforcement

Local law enforcement partners play a vital role in protecting the homeland and DHS provides a large number of resources to support that effort. Routine Sharing of USCIS data with local law enforcement agencies is compatible with the purpose of the system because local law enforcement are able to carry out their respective enforcement responsibilities and so that USCIS ensures that benefits or not granted to those who are not eligible due to law enforcement, public safety, or national security concerns. Routine Use G, N, and Q of the A-File SORN permits the sharing of information for the purpose of investigation or prosecuting investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on

its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations.

6.3 Does the project place limitations on re-dissemination?

USCIS, ICE, and CBP enters into Memorandum of Understanding/Agreement (MOU/A) with external organizations prior to the systematic sharing of information. When sharing information with parties outside of DHS, the same specifications related to security and safeguarding of privacy-sensitive information that are in place for USCIS and DHS are applied to the outside entity. The agreements between DHS and external entities fully outline the responsibilities of the parties, security standards and safeguarding responsibilities, and limits on the use of the information, including re-dissemination. Access to records is governed by need-to-know criteria that demand the receiving entity demonstrate the mission-related need for the data before access is granted. All Agreements contain language the legal authorization for the provision of the information to an external agency and the justification for the collecting of the data by the receiving agency. In addition, agreements contain an acknowledgement that the receiving agency will not share the information without USCIS or DHS's permission, as applicable.

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

USCIS keeps an electronic record of all CIS records shared via CIS and PCQS. TRKS, a subsystem of CIS, maintains an audit trail of the activities performed by CIS users. The audit trail includes any additions, deletions, or modifications, along with recording the viewing of selected information. PCQS also maintains audit trail logs to identify transactions performed by external users and transactions that involve external interconnected systems.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that data shared by USCIS with external partners will be used beyond the original purpose of collection (immigration benefits).

Mitigation: Information Sharing Agreements with external agencies contain specific requirements limiting access to those purposes set forth in the agreements. USCIS, ICE, and CBP all require privacy and security safeguards in established MOU/A with the external partners. When sharing information with parties outside of DHS, the same specifications related to security and safeguarding privacy-sensitive information that are in place for USCIS, ICE, and CBP are applied to the outside entity. The agreements between DHS and external entities fully outline responsibilities of the parties, security standards, and limits of use of the information, including re-dissemination, prior to information sharing. Access to records is governed by need-to-know criteria that demand the receiving entity demonstrate the mission-related need for the data before access is granted. In the terms of a negotiated agreement or the language of an authorization

providing information to an external agency, USCIS includes justification for collecting the data, and an acknowledgement that the receiving agency will not share the information without USCIS or DOS's permission, as applicable. All prospective information handlers must be authorized to access the information. This mitigates the risk of unauthorized disclosure by requiring a trained employee with access to the information to review the information before sharing the information with an external agency.

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?

An individual may gain access to his or her USCIS records by filing a Privacy Act or Freedom of Information (FOIA) request. Only U.S. citizens and lawful permanent residents may file a Privacy Act request. Any person, regardless of immigration status, may file a FOIA request. If an individual would like to file a Privacy Act or FOIA request to view his or her USCIS record, he or she may mail the request to the following address:

National Records Center
FOIA/Privacy Act Program
P. O. Box 648010
Lee's Summit, MO 64064-8010

Further information about Privacy Act/FOIA requests for USCIS records is available at http://www.uscis.gov.

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

U.S. citizens and lawful permanent residents, under the Privacy Act, are afforded the ability to correct information by filing a Privacy Act Amendment. U.S. citizens and lawful permanent residents should submit requests to contest or amend information contained in CIS as discussed in Section 7.1. The requestor should clearly and concisely state the information being contested, the reason for contesting or amending it, the proposed amendment, and any evidence of the correct information. The requestor should also clearly mark the envelope, "Privacy Act Amendment Request." The record must be identified in the same manner as described for making a request for access.

Persons not covered by the Privacy Act are also able to amend their records. If a person finds inaccurate information in his or her record received through FOIA, he or she may visit a local USCIS Field Office to identify and amend inaccurate records with evidence.

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

USCIS notifies individuals of the procedures for correcting their information on USCIS forms, the USCIS website, this PIA, and A-File SORN.

7.4 Privacy Impact Analysis: Related to Redress

There is no privacy risk related to redress. Individuals may request access to information about themselves under the FOIA and Privacy Act. USCIS also provides several avenues for individuals to correct inaccurate or erroneous information during and after the benefit decision.

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?

USCIS ensures that practices stated in this PIA comply with internal USCIS policies, including the USCIS privacy policies, standard operation procedures (SOP), orientation and training, rules of behavior, and auditing and accountability.

CIS has an audit trail capability to monitor user activities and generate alerts for unauthorized access attempts. Through TRKS, CIS is able to log the activity of each user to reduce the possibility of misuse and inappropriate dissemination of information. The audit trail includes any additions, deletions, or modifications CIS on-line and batch users perform, along with recording the viewing of selected information.

Additionally, USCIS uses the Restricted Access Management Tool (RAMT) to monitor and track users who were provide restricted access to TRKS across USCIS, ICE, and CBP in 148 FCO. Restricted Access is a set of privileges that allow authorized users to add or change critical data fields in CIS. RAMT is an automated tool that enables USCIS to monitor and track TRKS restricted access across all FCOs in near real time.

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

USCIS employees and contractors are required to complete annual Privacy and Computer Security Awareness Training to ensure their understanding of proper handling and securing of PII. Privacy training addresses appropriate privacy concerns, including Privacy Act obligations (*e.g.*, SORNs, Privacy Act Statements). The Computer Security Awareness Training examines appropriate technical, physical, and administrative control measures. Leadership at each USCIS office is responsible for ensuring that all federal employees and contractors receive the required annual Computer Security Awareness Training and Privacy training.

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

A USCIS deploys user role-based access controls and enforces a separation of duties to limit access to only those individuals who have a need-to-know in order to perform their duties. Each user role is mapped to the set of system authorizations required to support the intended duties of the role. The mapping of roles to associated authorizations enhances adherence to the principle of least privilege. Authorized users are broken into specific classes with specific access rights. This need-to-know is determined by the respective responsibilities of the employee. These are enforced through DHS and USCIS access request forms and procedures.

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?

USCIS has a formal review and approval process in place for new sharing agreements. Any new use of information and/or new access requests for the system must go through the USCIS change control process and must be approved by the proper authorities of this process, which includes the DHS and USCIS Privacy Officer, Chief Information Security Officer, Office of Chief

Counsel, and the respective Program Office.

Responsible Officials

Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

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