



Privacy Impact Assessment

for the

Person Centric Identity Services (PCIS) Initiative

DHS Reference No. DHS/USCIS/PIA-087

December 7, 2022



**Homeland
Security**



Abstract

U.S. Citizenship and Immigration Services (USCIS), a component of the U.S. Department of Homeland Security (DHS), is implementing Person Centric Identity Services (PCIS), an agency-wide effort to use enhanced business processes and emerging technologies to improve the reliability, accuracy, and completeness of biographic and biometric information across USCIS and other DHS immigration-related systems. The PCIS system compiles and aggregates this declared and obtained data through the use of algorithms and other sophisticated tools to establish an identity profile. The identity profile presents a single data set of consistent information about an individual's identity history as essential support for adjudicative efficiency.

There are limitations inherent in the current USCIS process of linking declared identity data solely to an individual's assigned identifier, which can lead to incomplete or unreliable records. To improve completeness and reliability, USCIS is leveraging existing Information Technology (IT) systems and using PCIS to enhance identity management across USCIS and other DHS components that rely on immigration records to accomplish their missions. Organizing and managing identity data in a "person centric" manner requires aggregating biometric data, biographic information, immigration status, and immigration history into a single identity profile. These profiles are stored in the Identity Index. This means that an individual's identity data is uniquely and accurately compiled so that each immigration benefit application, petition, or request, submitted to USCIS, each encounter with DHS¹ through administrative immigration proceedings before the U.S. Department of Justice (DOJ),² and any visa information collected by the U.S. Department of State (DOS),³ is accurately associated with that individual. The initial version of PCIS was released into production in November 2021 and consisted of the Identity Population Pipeline, the Identity Index, Core Search, and User Interface basic functions. USCIS is publishing this Privacy Impact Assessment (PIA) to describe the overall approach and vision for PCIS, as well as the personally identifiable information it plans to collect, use, maintain, and share. USCIS is developing PCIS in incremental phases and plans to update this PIA, as appropriate, to assess the privacy risks associated with future development efforts.

Overview

USCIS is the component of DHS that oversees adjudication of most requests for immigration benefits that grant a lawful immigration status in the United States. The mission of USCIS includes receiving and adjudicating a wide variety of immigrant and non-immigrant

¹ An "encounter with DHS" includes encounters with DHS components, such as the U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP).

² The DOJ Executive Office for Immigration Review handles immigration court proceedings.

³ DOS may need DHS information for purposes such as visa adjudications and consular reviews.



benefits, requests, and services (hereafter, *immigration benefit requests*).⁴ In carrying out its mission, USCIS and its predecessors have historically collected a significant amount of personal information from the individuals requesting immigration benefits and relied on paper-based processes to receive and adjudicate submitted immigration benefit requests. To index its records effectively, legacy Immigration and Naturalization Service issued unique A-Numbers⁵ and created associated individual files called A-Files.⁶

The Immigration and Naturalization Service introduced A-Files to streamline its recordkeeping. Prior to creating permanent physical A-Files, many individuals had more than one paper file in multiple locations within legacy the Immigration and Naturalization Service. In order to access all agency records for a particular individual, Immigration and Naturalization Service personnel were often required to search multiple file rooms, records systems, and indexes. By issuing A-Numbers, the Immigration and Naturalization Service created a single method to identify relevant files and records for unique individuals. A-Files and A-Numbers provided a straightforward mechanism for organizing paper records.

INS oversaw the immigration process, enforcement, and border patrol activities for seventy years until Congress passed the Homeland Security Act of 2002.⁷ With the creation of the U.S. Department of Homeland Security, the legacy Immigration and Naturalization Service functions are now shared between U.S. Citizenship and Immigration Services (USCIS), Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), and the DOJ Executive Office for Immigration Review. On March 1, 2003, USCIS assumed responsibility for the immigration service functions of the federal government. USCIS was founded to enhance the

⁴ Immigration benefit request/requestor. For purposes of this document, the term “immigration benefit request” includes all benefit requests (as defined in 8 C.F.R. § 1.2) as well as other immigration-related requests handled by USCIS that are not considered benefits—e.g., deferred action. The term “requestor” means someone who has filed an immigration benefit request.

⁵ An A-Number is a unique personal identifier assigned to individuals, including but not limited to individuals seeking immigration-related benefits, individuals who are under investigation for immigration violations, and for immigration-related enforcement actions. A-Files became the official files for all immigration and naturalization records created or consolidated since April 1, 1944, and “contain information regarding the transaction of an individual as [they pass] through the U.S. immigration process.” See DHS/USCIS/ICE/CBP-001 Alien File, Index and National File Tracking Systems of Records, 82 FR 43556 (Sept. 18, 2017), available at <https://www.dhs.gov/system-records-notices-sorn> (hereinafter “A-File SORN”).

⁶ The A-File contains records involving individuals as they pass through the U.S. immigration and inspection process. The A-File chronicles interactions, including Immigration and Nationality Act enforcement actions, with the U.S. Government. Previously the legacy Immigration and Naturalization Service performed all of these functions, but with the creation of the U.S. Department of Homeland Security those functions are now shared within DHS between USCIS, ICE, CBP, and also with the DOJ Executive Office for Immigration Review. The A-File does not typically contain records relating to temporary immigration benefits, such as extensions of authorized stay to temporary visitors for business or pleasure. Such records are maintained in Receipt Files for the period articulated in the relevant retention schedule. Receipt Files are not associated with an A-Number unless they relate to applications for permanent immigration benefits.

⁷ Pub. L. No. 107–296, 116 Stat. 2135.



security and efficiency of national immigration services by focusing exclusively on the administration of benefit applications. The Homeland Security Act also created ICE and CBP to oversee immigration enforcement and border security.

USCIS is the custodian of the A-File, which includes records that originate from USCIS, ICE, and CBP.⁸ The A-file may also contain records created during removal proceedings, which are administered by the DOJ Executive Office for Immigration Review, as well as records created by DOS as part of the consular visa application adjudication process. USCIS, ICE, CBP, the DOJ Executive Office for Immigration Review, and DOS contribute information to A-Files and use the records contained therein.⁹ USCIS also holds A-File content in various electronic repositories and case management systems¹⁰ used across product lines and agency divisions to complete adjudications. ICE, CBP, DOS, and eventually the DOJ Executive Office for Immigration Review will transition to contributing their respective records content electronically to USCIS,¹¹ rather than via paper, consistent with and supported by information-sharing agreements.

In accordance with USCIS' mission, USCIS interacts with applicants, petitioners, requestors, and beneficiaries as well as representatives, interpreters, preparers, sponsors, civil surgeons,¹² and others.¹³ USCIS associates paper and electronic case records to an immigration benefit requestor using A-Numbers. USCIS is engaged in an ongoing modernization effort that continues to use various unique identifiers, such as online account numbers, receipt numbers, and A-Numbers, to organize agency records, whether paper or electronic. While the methodology of using the assigned personal identifiers to accurately and efficiently organize paper and electronic

⁸ DHS primarily maintains information relating to the adjudication of benefits, investigation of immigration violations, and enforcement actions in A-Files. *See* A-file SORN. Note that the categories of records covered by the A-File SORN are more expansive than just those records submitted by individuals requesting immigration benefits.

⁹ *See* A-file SORN, at p. 43557.

¹⁰ USCIS electronic repositories and case management systems include: USCIS's Electronic Immigration System, Electronic Data Management System, and Content Management Service, Case and Activity Management for International Operations, and Investor File Adjudication Case Tracker.

¹¹ CBP is currently contributing electronic content to Content Management Service/STACKS as part of the Southwest border initiative. ICE and EOIR will also be contributing electronic content in the near future. For additional information about the Content Management Service, *see* U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CONTENT MANAGEMENT SERVICES (CMS), DHS/USCIS/PIA-079 (2019), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

¹² A civil surgeon is a physician designated by USCIS to conduct immigration medical examinations for individuals applying for an immigration benefit in the United States. For more information, please visit <https://www.uscis.gov/tools/designated-civil-surgeons>.

¹³ As a general matter, USCIS does not create an A-Number for native-born U.S. Citizens. However, in the event that a native-born person decides that they no longer wish to be a U.S. citizen, they may formally renounce their citizenship at an embassy or consulate outside of the United States. Once the individual renounces their U.S. citizenship, the DOS will send a Certificate of Loss of Nationality to USCIS and USCIS will create an A-File to house the Certificate of Loss of Nationality. Additionally, A-Files may be created for native-born U.S. Citizens who violate the nation's immigration laws.



content is reliable, consolidating all records for any individual into a single location has proven to be challenging over the years.

USCIS, ICE, CBP, the DOJ Executive Office for Immigration Review, and DOS each maintain respective records systems. These caches of transaction-based, personal data are created and maintained in a decentralized environment, scattered across multiple immigration systems. Although all of this immigration data in U.S. Government systems pertains to specific persons, a holistic view of any individual's unique immigration history is difficult to present, review, or analyze because the information and data is neither aggregated nor readily associated with a specific identity. The difficulty in efficiently obtaining a consolidated, cohesive, and accurate historical view of an individual's immigration information has resulted in the issuance of multiple A-Numbers to the same individual, the association of multiple individuals to a single A-Number, and inaccurate or out-of-date information.

USCIS is modernizing how it handles, obtains, stores, and analyzes identity data. These changes will increase efficiency of A-File records use and management for all government stakeholders, including ICE and CBP, as well as DOS and the DOJ Executive Office for Immigration Review, by increasing accurate and thorough association of an individual's identity information with their unique immigration records. The goal is to provide reliable, complete, and accurate information about USCIS immigration benefit requestors, and individuals suspected of violating U.S. immigration laws, and to improve the accuracy of how an individual's immigration records and encounters are organized and managed. This is accomplished by:

- Improving data integrity by ensuring identity data is accurate and each immigration benefit requestor or suspected immigration law violator is assigned a unique identifier (which is randomly generated);
- Enhancing the use of biographic entity resolution techniques through machine learning technology as well as conformance to DHS data standards to better match immigration benefit requests and encounter records to unique individual identities; and
- Implementing a standardized person centric data structure as it relates to immigration information derived from immigration benefit requests and enforcement actions.

Although the A-File SORN covers several components (USCIS, ICE and CBP), USCIS is the custodian of the A-file and is therefore primarily responsible for managing it. Part of this responsibility is ensuring the records contained in each A-File are associated with the correct individual. USCIS also uses several case management and other record systems that contain person data, including but not limited to, Central Index System 2,¹⁴ Customer Profile Management

¹⁴ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CENTRAL INDEX SYSTEM (CIS), DHS/USCIS/PIA-009 (2009 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.



System,¹⁵ USCIS Electronic Immigration System,¹⁶ Computer Linked Application Information Management System 3,¹⁷ Global (Not an Acronym),¹⁸ the Investor File Adjudication Case Tracker,¹⁹ Case and Activity Management for International Operations,²⁰ Content Management Service,²¹ National Appointment Scheduling System,²² to administer, process, and adjudicate immigration benefit requests. Each of these systems maintains separate and different records on the subject individual.

CBP uses and contributes to the A-File to accomplish its mission to enforce the nation's immigration laws at and between the nation's ports of entry.²³ In addition to physical A-File records, CBP uses the e3 portal to collect and transmit biographic, encounter, and biometric data of individuals encountered by U.S. Border Patrol. U.S. Border Patrol agents enforce immigration and customs laws between the nation's ports of entry, detecting, interdicting, and apprehending those who attempt to illegally enter the United States or smuggle individuals or contraband into the United States, and prevent the entry of terrorists and terrorist weapons. The e3 portal was

¹⁵ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CUSTOMER PROFILE MANAGEMENT SERVICE (CPMS), DHS/USCIS/PIA-060 (2015 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁶ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC IMMIGRATION SYSTEM, DHS/USCIS/PIA-056, (2018 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁷ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE COMPUTER LINKED APPLICATION INFORMATION MANAGEMENT SYSTEM (CLAIMS 3) AND ASSOCIATED SYSTEMS, DHS/USCIS/PIA-016(a) (2008 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁸ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ASYLUM DIVISION, DHS/USCIS/PIA-027(c) (2009 and subsequent updates), available at: <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁹ See forthcoming EB-5 Program PIA.

²⁰ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CASE AND ACTIVITY MANAGEMENT FOR INTERNATIONAL OPERATIONS (CAMINO), DHS/USCIS/PIA-051 (2020 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

²¹ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CONTENT MANAGEMENT SERVICES (CMS), DHS/USCIS/PIA-079 (2019), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

²² See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR CUSTOMER SCHEDULING AND SERVICES, DHS/USCIS/PIA-046 (2014 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

²³ CBP is responsible for securing America's borders to protect the United States against terrorist threats and to prevent the illegal entry of inadmissible persons and contraband, while also facilitating lawful travel, trade, and immigration. CBP's U.S. Border Patrol is responsible for protecting the Nation by reducing the likelihood that dangerous people enter the United States *between* the ports of entry. CBP's Office of Field Operations is responsible with ensuring compliance with federal laws *at* ports of entry, including preventing inadmissible persons from entering or exiting the United States.



established to generate certain immigration enforcement forms, capture signatures from U.S. Border Patrol agents and individuals in custody, capture U.S. Border Patrol agent narratives entered by U.S. Border Patrol agents and transmit biographic information to various systems.²⁴ Many but not all of the U.S. Border Patrol records and associated person data are also A-File content.

CBP also uses and contributes to the A-File during the traveler inspection process at United States ports of entry. CBP officers conduct primary inspections to determine whether travelers and their belongings are admissible and whether there are any violations of the laws CBP is authorized to enforce or administer at the border. If additional inspection is required, CBP officers use Unified Secondary, a consolidated inspection and immigration events processing tool to complete the secondary inspection.²⁵ Similar to the information that U.S. Border Patrol agents collect and input into e3, the information collected and generated into Unified Secondary during the secondary inspection is A-File content. CBP's Arrival and Departure Information System aggregates biographic, biometric indicator, and travel data on all travelers. ADIS is accessed and used to assist in determining visa or immigration benefits eligibility and supporting law enforcement investigations.²⁶

ICE also uses the Enforcement Integrated Database, a repository for software applications (collectively referred to as the ENFORCE applications) to capture and maintain information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and law enforcement investigations and operations, to assist in carrying out its law enforcement duties.²⁷

USCIS, ICE, and CBP systems will submit person data relating to A-File content for PCIS to store in a single centralized location, called the Identity Index. The Identity Index currently stores historic person data gathered from USCIS case management and other systems relied upon to adjudicate immigration benefit requests. USCIS, ICE, and CBP are currently coordinating efforts to include e3 and Unified Secondary information in the Identity Index to create a

²⁴ See U.S. DEPARTMENT OF HOMELAND SECURITY, CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE CBP PORTAL (E3), DHS/CBP/PIA-012(c) (2021), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

²⁵ See U.S. DEPARTMENT OF HOMELAND SECURITY, CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE U.S. CUSTOM AND BORDER PROTECTION UNIFIED SECONDARY, DHS/CBP/PIA-067 (2021), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

²⁶ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, DHS/CBP/PIA-024 Arrival and Departure Information System (2007 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

²⁷ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2010 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-ice>.



comprehensive, person-centric view of individuals. Although PCIS receives identity information stemming from A-File content, PCIS is not the same as the A-File. PCIS is intended to provide a comprehensive, person-centric view of a person in order to better associate all relevant A-File content with the correct identity, regardless of the content's location or medium (i.e., paper, electronic, or hybrid paper/electronic). Not all contributors of A-File content will use PCIS, though the identity-related information they provide may be incorporated into PCIS. Currently, only USCIS, ICE, and CBP use PCIS.²⁸

Additionally, the DHS Office of Intelligence and Analysis (I&A) will access PCIS in support of its mission, which includes identifying "U.S. Persons," defined as United States citizens, Lawful Permanent Residents, unincorporated associations substantially composed of United States citizens or permanent resident non-citizens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.²⁹ I&A is authorized to collect, retain, or disseminate information concerning "U.S. persons" only in accordance with procedures approved by the Attorney General.³⁰ Therefore, using PCIS to assist in determining a person's immigration status is important to their mission.

DOS has also requested PCIS access to support its mission of adjudicating overseas visa applications submitted by individuals, including those who are the beneficiaries of immigrant and non-immigrant visa petitions. DOS relies on accurate A-Number and identity information to determine whether the individuals DOS processed overseas for visa issuance are the same individuals associated with USCIS records, if any. PCIS will support DOS by providing automated A-Number validation and issuance services, as described below. As such, use of PCIS will result in a reduction in issuing duplicate A-Numbers to the same unique individuals or the re-issuance of the same A-Number to multiple different individuals.³¹ The initial version of PCIS was released into production in November 2021 and consisted of the Identity Population Pipeline, the Identity Index, Core Search, and User Interface basic functions. USCIS has continued to implement additional functions. Currently, PCIS consists of the following services:

²⁸ Should any other agencies receive access to PCIS, USCIS will update this PIA.

²⁹ See E.O. 12333, *United States Intelligence Activities*, 2008 as amended.

³⁰ See *Department of Homeland Security Office of Intelligence and Analysis Instruction IA-1000*, January 19, 2017, available at <https://www.dhs.gov/sites/default/files/publications/office-of-intelligence-and-analysis-intelligence-oversight-program-and-guidelines.pdf>.

³¹ See U.S. DEPARTMENT OF STATE, CONSULAR AFFAIRS, CONSULAR CONSOLIDATED DATABASE (CCD) PRIVACY IMPACT ASSESSMENT (2015 and subsequent updates), available at <https://www.state.gov/privacy-impact-assessments-privacy-office/>.



- **Identity Population Pipeline.** The Identity Population Pipeline is the mechanism in which replicated data from USCIS source systems³² (*Central Index System 2*,³³ *Change of Address Card (AR-11)*,³⁴ *Customer Profile Management System*,³⁵ *Global*,³⁶ *USCIS Electronic Immigration System*,³⁷ *Computer Linked Application Information Management System 4*,³⁸ *System 3 (CLAIMS3)*, *the Investor File Adjudication Case Tracker*,³⁹ *Investor File Adjudication Case Tracker*,⁴⁰ and *Case and Activity Management for International Operations*⁴¹) are ingested from the Enterprise Citizenship and Immigrations Services Centralized Operational Repository database information system “data lake,”⁴² conformed to DHS and USCIS standards, and matched together using a weighted absolute scoring model and a machine-learning model to associated the aggregated data to a unique identity. The Identity Population Pipeline was used to populate PCIS with all the historical records (approximately one-half billion) from the USCIS source systems and is also continuously

³² Currently, eight systems source the data used in PCIS. However, over time, the list will change as systems are replaced, updated, or decommissioned.

³³ Central Index System serves as a DHS-wide index to track the history of an immigrant and non-immigrant in the adjudication process, as well as the location of immigration case files.

³⁴ Change of Address Card (AR-11) tracks address changes submitted to DHS as required by section 265 of the Immigration and Nationality Act, 8 U.S.C. § 1305.

³⁵ Customer Profile Management Service serves as a person-centric repository of biometric and biographic information provided by applicants and petitioners (hereafter collectively referred to as “benefit requestors”) who have been issued a USCIS card evidencing the granting of an immigration-related benefit (i.e., permanent residency, work authorization, or travel documents).

³⁶ Global is a comprehensive case management tool that enables USCIS to process applications for asylum pursuant to section 208 of the Immigration and Nationality Act, and applications for suspension of deportation or special rule cancellation of removal pursuant to the Nicaraguan Adjustment and Central American Relief Act (“Nicaraguan Adjustment and Central American Relief Act 203”).

³⁷ USCIS Electronic Immigration System is an electronic case management system that allows USCIS to process certain immigration benefits requests.

³⁸ Computer Linked Application Information Management System 4 was used to process applications for naturalization and citizenship. Computer Linked Application Information Management System 4 was decommissioned in 2020. Data are historically available within the Enterprise Citizenship and Immigrations Services Centralized Operational Repository.

³⁹ Computer Link Application Information Management System is used to manage the adjudication process for most domestically-filed, paper-based immigration benefit filings with the exception of naturalization, intercountry adoptions, and certain requests for asylum and refugee status.

⁴⁰ Investor File Adjudication Case Tracker supports the case management/review functions of the Fifth Preference Employment-Based Immigration Visa (EB-5) Program. Adjudicators use Investor File Adjudication Case Tracker to manage information and record adjudicative actions taken on each case and update case information for Regional Centers, New Commercial Enterprise, Job Creating Enterprise, attorney and firm information, associated Job Creating Enterprise s’ with New Commercial Enterprises’.

⁴¹ Case and Activity Management for International Operations is used to track the processing of immigration applications and petitions received or adjudicated by Refugee, Asylum, and International Operations.

⁴² Enterprise Citizenship and Immigrations Services Centralized Operational Repository is a collection of databases that serves as both a data warehouse and data hub for systems requiring data from other systems for operations. [See PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE CITIZENSHIP AND IMMIGRATION SERVICES CENTRALIZED OPERATIONAL REPOSITORY \(eCISCOR\), DHS/USCIS/PIA 0-23\(b\), July 26, 2018, available at https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-023b-eciscor-oct2019.pdf.](https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-023b-eciscor-oct2019.pdf)



used to capture new data (e.g., new applications) as well as changes in the source systems' data. The Identity Population Pipeline delivered the capability to aggregate historical as well as new USCIS records under unique identities.

- **The Identity Index.** The Identity Index is the core of PCIS where identity data of applicants and beneficiaries are stored and aggregated, along with their corresponding transactional records, such as immigration benefit requests. The Identity Index assigns an Identity ID and stores this information to allow the search and retrieval of data associated with a unique identity and the history of the transactions that represent the end-to-end immigration lifecycle for that individual.
 - **Verification Services.** The Verification Services enables USCIS' Verification Information System to call the PCIS Identity Index to retrieve person-centric identity information. This service will provide USCIS' Verification Information System with class of admission and work authorization provision of law information as well as employment authorization history that will be used by the Systematic Alien Verification for Entitlements⁴³ and E-Verify⁴⁴ Programs. Systematic Alien Verification for Entitlements will use this information to provide naturalized U.S. citizenship and immigration status information of benefit applicants to federal, state, and local benefit granting agencies to determine their applicant's eligibility for the benefits and licenses they administer. The E-Verify Program will use the employment authorization information to confirm employment eligibility for employers who participate in the program.
- **Core Search.** Core Search is the standard way systems can integrate with PCIS to query and retrieve person centric information from the Identity Index. PCIS will consistently provide an accurate identity based upon a variety of query inputs (i.e., identifiers, biographic, and biometric data). The Core Search service can be integrated with other systems to support multiple operations or workflows and provide customized responses that are tailored for that intended purpose. For example, a query from a Case Management System using Receipt Number, Name, and date of birth to return the most updated address information for an identity could be performed using this service.

⁴³ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE SYSTEMATIC ALIEN VERIFICATION FOR ENTITLEMENTS PROGRAM, DHS/USCIS/PIA- DHS/USCIS/PIA-006(c) (2020), available at <https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis006c-save-july2020.pdf>.

⁴⁴ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE E-VERIFY PROGRAM, DHS/USCIS/PIA- DHS/USCIS/PIA-030(g) (2019), available at <https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhsuscis030ge-verifynlets-june2019.pdf>.



- **Identity Resolution Queue.** When discrepancies in data consistency are recognized within an identity profile or with a newly ingested transaction, PCIS relies on the Identity Resolution Queue to allow internal users to recommend changes to the data believed to be inaccurate. The Identity Resolution Queue is addressed by a human Identity Specialist who reviews and approves or denies the inbound transactions in source systems.
- **File/Record Management Services.** PCIS will integrate with other immigration record systems to provide a person-centric user experience.
 - **Content Management Services and STACKS (Not an Acronym).**⁴⁵ Content Management Service-STACKS (commonly referred to as STACKS) is the user interface that allows USCIS users to view file content within Content Management Service. USCIS staff use STACKS to view digital A-File records, immigration benefit requests, evidence, and other case content that is stored digitally within Content Management Service. STACKS will integrate with PCIS to display the identity data associated with digital records viewable within the STACKS user interface.
 - **RAILS (Not an Acronym).**⁴⁶ RAILS is an automated file system that tracks internal immigrant files and receipt files and allows for certain DHS users to request immigration files. RAILS enables USCIS to electronically maintain an accurate file inventory, track the location of paper and electronic immigration files via a web-based system and/or mobile application, and allows users to order, transfer, and receive official paper and electronic immigration records related to the A-Number). RAILS will integrate with PCIS to associate all A-Files belonging to an individual so that end users will be informed of each file's location and be able to request all records related to the same person. In addition, PCIS will implement a PCIS File Location service that will present the file location information within the PCIS User Interface and broker the data as needed to other integrating systems.
- **User Interface.** The PCIS User Interface is a web-based user interface that provides access, using single sign-on, allowing users to search the Identity Index for a unique identity using operational identifiers or biographic attributes using fuzzy match logic;⁴⁷ view an organized summary view of the identity based on the primary values for each attribute (e.g.,

⁴⁵ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CONTENT MANAGEMENT SERVICES (CMS), DHS/USCIS/PIA-079 (2019), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

⁴⁶ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR RAILS, DHS/USCIS/PIA-075 (2018), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

⁴⁷ Fuzzy match logic is a strong algorithm used to determine a match confidence level from the immigration benefit request form and the information the A-Number validation microservice receives from USCIS source systems.



primary name, primary data of birth), view all (historical and new) person data associated with the identity, along with their lineage (e.g., the originating immigration form type, benefit request receipt number, and associated source system); and view the immigration history⁴⁸ of the individual. The PCIS User Interface provides the following capabilities to its users:

- **Identifier Search.** Search input that allows users to quickly input one of the three most frequently used identifiers to search (Fingerprint Identification Number, receipt, or A-Number) without need to designate the identifier type.
- **Advanced Search.** Search input that allows users to conduct more targeted search by using combinations of identifiers currently supported by PCIS, including first name, last name, middle name, date of birth (with a range in future), A-Number country of birth, country of citizenship, fingerprint identification number, form I-94 arrival/departure record, USCIS online account number, foreign passport number, USCIS receipt number, encounter ID, and Social Security number.
- **Identity View.** The PCIS Identity View employs business rules⁴⁹ to select the best representative data from all of the transactions associated to a person to create the PCIS Identity View. The PCIS Identity View provides users with the most relevant identity, immigration, and contact information.
- **Additional Information View.** Provides users with a view of each of the transactions that PCIS ingested through the Identity Population Pipeline and matched to the unique identity. The transactions are shown in a table format containing the conformed values ingested for each transaction.
- **Customer Profile Management System Background Check.** Provides PCIS users with background check information derived from biometric and biographic data and available to other case management systems through direct system integration with the Customer Profile Management System. Results from background checks would be provided from the following databases, as appropriate: FBI Response, Automated Biometric Identification System, watchlist status, and FBI Namecheck.
- **Immigration Timeline View.** Uses the Identity Population Pipeline data weighing and matching methodology and presents relevant data from other federal government immigration systems outside of USCIS to provide a timeline of immigration activities associated with an identified unique identity. The timeline

⁴⁸ All records, from the eight source systems, associated with the individual plus records created in e3, Unified Secondary, and Unified Immigration Portal.

⁴⁹ Business rules are established criteria in the system that determine how a process is performed by the system.



currently includes all transactions ingested and matched from USCIS source systems, as well as benefit cards, biometric events from the Automated Biometric Identification System (IDENT),⁵⁰ and Visa Applications from DOS Consular Consolidated Database. While still currently in development, PCIS plans to connect to the following systems to provide the most comprehensive immigration timeline view for an individual:

- **CBP – Arrival and Departure Information System.**⁵¹ The Arrival and Departure Information System contains records of entry and exit through United States air, land, and seaports. PCIS will use assigned identifiers (e.g., Fingerprint Identification Number, A-Number) to query the Arrival and Departure Information System and integrate the response events into PCIS as part of the immigration timeline view. PCIS will query the web service offered by Arrival and Departure Information System to retrieve the arrival and departure data in real time to display alongside identity information. CBP’s Arrival and Departure Information System maintains records of entry and exit border crossings, which is important information when adjudicating benefits to validate in-country requirements and validate travel history provided by the applicant. By querying CBP Arrival and Departure Information System for an identity and integrating the response into the PCIS immigration timeline, PCIS will provide a more complete immigration timeline to users.
- **Department of Justice (DOJ) Executive Office of Immigration Review.** PCIS will connect to and query Executive Office of Immigration Review data based on technical parameters set by the DOJ Executive Office for Immigration Review service. By querying the DOJ Executive Office for Immigration Review, PCIS will present an individual’s immigration court history and include this information in the Immigration Timeline view.
- **CBP TECS.**⁵² A TECS subject query retrieves biographic data about individuals who have been encountered by DHS in an immigration, law

⁵⁰ See U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-001 (2012), available at <https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim>.

⁵¹ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION (CBP), PRIVACY IMPACT ASSESSMENT FOR THE ARRIVAL AND DEPARTURE INFORMATION SYSTEM (ADIS), DHS/CBP/PIA-024 (2007 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

⁵² See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION



enforcement, or anti-terrorism context, as well as information about known or suspected violators who are DHS subjects of interest and include biographic, passport, border crossing, inspection, visa, and nonimmigrant arrival and departure information. PCIS will display TECS information related to adjudicating their immigration or enforcement case.

- **CBP Automated Targeting System.**⁵³ 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. ATS processes biographical data collected from travelers (e.g., passengers and crewmembers) entering and exiting the United States primarily through air and seaports and is used to establish immigration status, as well as to assist in performing risk assessments for whether travelers should receive additional screening prior to entry or departure. By querying Automated Targeting System, PCIS will provide a comprehensive and person-centric view of an individual's immigration timeline view.
- **ICE Student and Exchange Visitor Information System.**⁵⁴ The Student and Exchange Visitor Information System is an Internet-based system that allows DHS to collect, maintain, and use accurate and current information on nonimmigrant students, their dependents, exchange visitors, and the approved schools and designated U.S. sponsors that host nonimmigrant students. By querying the Student and Exchange Visitor Information System, PCIS will provide users a comprehensive and person-centric view of an individual's immigration timeline view.
- **ICE Enforcement Integrated Database.**⁵⁵ As mentioned, ICE personnel use Enforcement Integrated Database and ENFORCE to support ICE's arrest of individuals for violating criminal laws enforced by ICE, as well as detaining, processing, and removing non-citizens in the United States who

(CBP), PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: PLATFORM, DHS/CBP/PIA-021 (2016), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

⁵³ See, U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION (CBP), PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM (ATS), DHS/CBP/PIA-006 (2007 AND SUBSEQUENT UPDATES), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

⁵⁴ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT (ICE), PRIVACY IMPACT ASSESSMENT FOR THE STUDENT AND EXCHANGE VISITOR PROGRAM (SEVP), DHS/ICE/PIA-001 (2020), available at <https://www.dhs.gov/privacy-documents-ice>.

⁵⁵ See Supra Note 27.



violate immigration laws. Querying ENFORCE will provide users a comprehensive and person-centric view of an individual's immigration timeline for either adjudicating immigration cases or for law enforcement purposes.

- **DOS Consular Consolidated Database.**⁵⁶ The Consular Consolidated Database is a DOS system used by consular personnel as a resource for verifying prior visa issuances and refusals for individuals seeking entry into the United States, as well as statistical reporting. Querying the Consular Consolidated Database will allow PCIS users to access an individual's visa information in a person-centric view and chronological immigration timeline view to better assist in making immigration case decisions.
- **Identity Validation Services.** Additional services that are provided by PCIS are the following:
 - **A-Number Validation.** Accepts declared information about a subject to include A-Number, Fingerprint Identification Number, names, date of birth, country of birth, country of citizenship, and other identifier and searches the PCIS Identity Index to find a data set reflecting the highest level of consistency for matching data. If a match is found then the primary A-Number, identifiers, and biographic information known to PCIS are returned to the requestor. This matching service determines which A-Number a subject should be processed under. PCIS is currently integrated with E3, USEC, and in progress with EAGLE for purposes of A-Number Validation. CBP and ICE will use this service to compare declared or collected information from a subject against the PCIS Identity Index. If a match is found, the primary A-Number, identifiers, and biographic information are returned to the requestor.
 - **A-Number Issuance.** Accepts a minimal set of biographic and biometric information⁵⁷ to issue a new A-Number for an individual. The new A-Number and information provided by a DHS component is recorded in Central Index System 2 and delivered to PCIS in near-real-time. Eventually PCIS will be expanded to permit the DOS to issue A-Numbers through PCIS as part of the DOS visa process. A-Number Issuance performs this same function for ICE and CBP, both of which

⁵⁶ See U.S. DEPARTMENT OF STATE, CONSULAR AFFAIRS, CONSULAR CONSOLIDATED DATABASE (CCD) PRIVACY IMPACT ASSESSMENT (2015 and subsequent updates), available at <https://www.state.gov/privacy-impact-assessments-privacy-office/>.

⁵⁷ At a minimum, the A-Number issuance service requires a first name, last name, date of birth, country of birth, form type, class of admission, and Fingerprint Identification Number to issue an A-Number for an individual.



also issue A-numbers to create A-files incident to immigration law enforcement encounters.

- **PCIS Enterprise Name Service.** Provides the name, alias, date of birth, and data source(s), such as the form, receipt number, and transaction date from which the names or aliases were derived.
- **Customer Profile Management System Vetting Service.** Provides an enhanced vetting service through the PCIS sophisticated logic to enable the re-use of individuals' previously collected biometrics. As such, this vetting service will increase Application Support Centers efficiency by allowing individuals to be scheduled for a shorter biometrics appointment. If the individuals' prints cannot be verified for some reason, the individual's fingerprints will be recaptured.
- **National Appointment Scheduling System Scheduling Service.** Integrations between PCIS and National Appointment Scheduling System will enhance the scheduling service to ensure USCIS schedules applicants in a person-centric manner so applicants are scheduled once (rather than multiple times) for each immigration benefit application. Additionally, this service will improve the grouping logic for family units.
- **Special Protected Class⁵⁸ Service.** Establishes a Special Protected Class service that provides the capability for all systems connected with PCIS (e.g., USCIS, CBP, ICE) to know whether any Special Protected Class banners should be displayed for a given individual. Special Protected Class banners alert users that a record relates to an identity whose data is subject to specific additional protections.

PHASED APPROACH FOR FUTURE PERSON CENTRIC CAPABILITIES

USCIS is moving in incremental phases using the agile systems development approach to implement person centric capabilities across the agency.⁵⁹ In the first phase, USCIS deployed the

⁵⁸ Special Protected Class, as used in this PIA, refers to individuals that are afforded additional privacy protections including asylees under 8 C.F.R. § 208.6 and refugees by policy. In addition, this term includes applicants and recipients of immigration relief under the Violence Against Women Act of 1994, Pub. L. 103-322, September 13, 1994, 108 Stat. 1796 (reauthorized on March 15, 2022) (VAWA) and T and U nonimmigrant status for victims of trafficking and other serious crimes.

⁵⁹ As the custodian of the A-File, USCIS manages access rights to electronic A-File content through policy and systems controls. As with the A-File, direct access to PCIS is limited to DHS personnel and approved contractors who have a need-to-know and access the records contained in the A-file to perform their duties. See A-File SORN, available at <https://www.dhs.gov/system-records-notices-sorns>, and 5 U.S.C. § 552(b)(1). USCIS will update this PIA to address access to PCIS and privacy protections if PCIS access is expanded to other federal agencies with a valid mission need-to-know.



A-Number Validation, Person Centric Entity Resolution,⁶⁰ A-Number Issuance, and Profile Manager microservices. These microservices enhanced existing processes by associating data from USCIS, DHS, and external source systems, performing data analysis using the associated data, and managing and resolving identities across systems.

Deploying the PCIS User Interface was the second phase of implementing person centric capabilities. As mentioned, the PCIS User Interface is web-based and displays a banner across the top of the screen that labels the data as a “Special Protected Class” as required by 8 U.S.C. § 1367 (Section 1367) and 8 C.F.R. § 208.6 (Section 208.6)⁶¹ protections, and provides “hotlist” search tracking.⁶² The features available to users at the minimum viable product level⁶³ include the ability for a user, such as an adjudicator, a USCIS Fraud Detection and National Security officer, Freedom of Information Act (FOIA) case analyst, and other authorized users, to login to PCIS, and in one place, search for an individual’s identity profile, and view the organized person data, records, and immigration history associated with that person. This is the first time that USCIS will have the full immigration history and current immigration status of a unique individual available to view in a simple, comprehensive, and organized manner. Although, with the minimum viable product offering, users must still use the PCIS User Interface as a separate system. Future access will be simplified when the PCIS User Interface is integrated into agency case management systems. Users will then be able to use the PCIS system without having to leave the case management system in which they were already working. This embedded and integrated approach will result in reduced processing times. Additionally, an overall increase in efficiency—such as case preparation, FOIA response production, and fraud research— as well as a reduction in processing

⁶⁰ Person Centric Entity Resolution is a more advanced and analytically intensive method of record matching than is generally used by USCIS systems when issuing A-Numbers, account numbers, or for matching individuals’ records. It incorporates established rules and machine learning to account for numerous types known and discoverable data discrepancies across data sets and provides more reliable record matching.

⁶¹ Federal regulations at 8 C.F.R. § 208.6 generally prohibit the disclosure to third parties of information contained in or pertaining to asylum applications, credible fear determinations, and reasonable fear determinations. These regulations safeguard information that, if disclosed publicly, could subject the claimant to retaliatory measures by government authorities or non-state actors in the event the claimant is repatriated. Such disclosure could also endanger the security of the claimant’s family members who may still be residing in the country of origin. As a matter of longstanding policy, the confidentiality protections in these regulations are extended to Registration for Classification as Refugee (Form I-590), Refugee/Asylee Relative Petitions (Form I-730), and Applications for Suspension of Deportation or Special Rule Cancellation pursuant to Nicaraguan Adjustment and Central American Relief Act (Form I-881). USCIS extended the confidentiality provisions under 8 C.F.R. § 208.6 to refugees by policy. See “Fact Sheet: Federal Regulation Protecting the Confidentiality of Asylum Applicants,” October 12, 2012, at pg.7.

⁶² The “hotlist” is an internal list maintained by USCIS records of high-profile individuals or public figures. Tracking queries by USCIS personnel on “hotlist” individuals is key to preventing curiosity browsing and misuse of systems by USCIS personnel.

⁶³ “Minimally Viable Product” refers to the basic functionality needed to have the system at an operable state and a platform upon which USCIS can iteratively incorporate additional functionality and enhancements to functionality based on user feedback.



times is generally expected for PCIS users who will be able to complete the search and analysis of multiple data sources in one search instead of multiple searches.

USCIS is conducting this PCIS Initiative PIA to provide transparency to the public about the overall concept and implementation of PCIS along with detailed information on each of the implemented Person Centric Service (PCS) microservices. Due to the continuously changing environment of PCIS, this PIA may require several addendums or updates. Therefore, USCIS will submit addendums to this PIA or PIA updates, as appropriate, to assess the privacy risks associated with the implementation of new or updated PCIS capabilities. Furthermore, USCIS will ensure that any use of data is consistent with applicable laws, DHS privacy principles and policies, and the purposes for which the information was originally collected as set forth in applicable System of Record Notices (SORNs).

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?

USCIS collects and uses immigration benefit request information under the authority of the Immigration and Nationality Act. Section 103 of the Immigration and Nationality Act, 8 U.S.C. § 1103, charges the Secretary of Homeland Security with the duty of administering and enforcing all laws relating to the immigration and naturalization of individuals. Specifically, 8 U.S.C. § 1360 requires the creation of a central file of information for the use of security and enforcement agencies of the government of the United States that contains the names of all aliens admitted or denied admission to the United States and such other relevant information as required to aid in the proper enforcement. All data ingested for purposes of PCIS have already been obtained and used for purposes that are consistent with USCIS authorities. PCIS supports the management of immigration records in a person-centric manner. USCIS, ICE, and CBP continue to use immigration records to adjudicate immigration benefit requests, for enforcement, and other decision-making processes. However, USCIS, ICE, and CBP can now use PCIS, together with other legacy systems, to analyze data and information (such as biographic, biometric information, and case history details) associated to unique individual identities. In time, as PCIS functionality grows, Central Index System 2, Person Centric Services, and Person Centric Query Service, and similar systems of record will be subsumed into or replaced by PCIS.

1.2 What Privacy Act SORN(s) apply to the information?

The information collected, used, maintained, and disseminated by the PCS microservices and PCIS are covered by the following SORNs:

- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System SORN, which covers the collection, use, and maintenance of applications and



supplemental evidence, in addition to other information related to the individual as they pass through the immigration process.⁶⁴

- DHS/USCIS-007 Benefit Information System SORN, which covers the collection and use of immigrant and non-immigrant request forms, decisional data, and associated fees for adjudication.⁶⁵
- DHS/USCIS-010 Asylum Information Prescreening SORN, which covers the collection, use, and maintenance of asylum applications, Nicaraguan Adjustment and Central American Relief Act § 203 applications, credible fear screenings, and reasonable fear screenings.⁶⁶
- DHS/USCIS-017 Refugee Case Processing and Security Screening Information SORN, which covers the collection, use, maintenance, and dissemination of refugee applications, to include application intake, biometric checks, interviews, and adjudication.⁶⁷
- DHS/USCIS-018 Immigration Biometric and Background Check SORN, which covers background checks and their results.⁶⁸
- DHS/USCIS-005 Inter-Country Adoptions Security SORN, which covers information collected during the intercountry adoptions process and includes all individuals seeking an intercountry adoption; any additional adult members of the household; representatives of the prospective adoptive parent(s); minors being adopted; and biological parents, or custodians of adopted minors, preparers, and adoption service providers.⁶⁹

While PCIS retrieves information from both USCIS systems and non-USCIS systems (i.e., CBP, ICE, DoS, and DOJ systems), only the information retrieved from USCIS systems is stored within

⁶⁴ DHS/USCIS/ICE/CBP-001 Alien File, Index, And National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017), available at <https://www.dhs.gov/system-records-notices-sorns>.

⁶⁵ DHS/USCIS-007 Benefits Information Systems System of Records, 81 FR 72069 (Oct. 19, 2016), available at <https://www.dhs.gov/system-records-notices-sorns>.

⁶⁶ DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (Nov. 30, 2015), available at <https://www.dhs.gov/system-records-notices-sorns>.

⁶⁷ DHS/USCIS-017 Refugee Case Processing and Security Screening Information System of Records, 81 FR 72075, (Oct. 19, 2016), available at <https://www.dhs.gov/system-records-notices-sorns>.

⁶⁸ DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, 83 FR 36950 (July 31, 2018), available at <https://www.dhs.gov/system-records-notices-sorns>.

⁶⁹ DHS/USCIS-005 Inter-Country Adoptions Security System of Records, 81 FR 78614 (November 8, 2016), available at <https://www.dhs.gov/system-records-notices-sorns>.



the PCIS Identity Index. Each non-USCIS system is covered by an appropriate Privacy Act System of Records Notice.⁷⁰

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

PCIS is a major application that is currently undergoing the Security Authorization Process and is in the Initiation Phase of this process. The primary goal of this Phase is to create the appropriate documentation, including this PIA. Upon completion of this PIA, PCIS will be able to proceed to the next phase of the Security Authorization Process and start with the Security Control Assessment. Once the Security Authorization Process is complete and the Security Authorization/Authority to Operate is granted, PCIS will be accepted into the Ongoing Authorization program which is intended to continuously monitor and maintain the security posture of the system.

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

PCIS does not collect new data, but instead retrieves already collected data from existing USCIS source systems for inclusion in the PCIS Identity Index. While PCIS retrieves information from both USCIS systems and non-USCIS systems to be presented to the user, only the information retrieved from USCIS systems is stored within the PCIS Identity Index. To create this comprehensive, person-centric view of individuals, PCIS includes data, system architecture, and user functionality from Central Index System 2, Person Centric Query Service, person data from USCIS case management systems, as well as integration with the Customer Profile Management System. NARA approved the Central Index System 2 retention schedule N1-566-10-01 on November 05, 2009. According to this retention schedule, Central Index System 2 records are permanent and USCIS transfers A-Files to the custody of NARA 100 years after the individual's date of birth. Furthermore, Customer Profile Management System data will be retained for 100 years from the individual's date of birth in accordance with NARA Disposition Authority Number DAA 0563-2013-0001-0005.

⁷⁰ CBP and ICE SORNs can be accessed through the DHS website; non-DHS SORNs can be accessed through the respective entity's website. While not an exhaustive list, these applicable SORNs include: [DHS/CBP-006 Automated Targeting System](#), 77 FR 30297 (May 22, 2012); [DHS/CBP-007 CBP Border Crossing Information](#), 81 FR 89957 (December 13, 2016); [DHS/CBP-011 U.S. Customs and Border Protection TECS](#), 73 FR 77778 (December 19, 2008); [DHS/CBP-021 Arrival and Departure Information System](#), 80 FR 72081 (November 18, 2015); [DHS/CBP-023 Border Patrol Enforcement Records \(BPER\)](#), 81 FR 72601 (October 20, 2016); [DHS/ICE-001 Student and Exchange Visitor Information System](#), 86 FR 69663 (December 8, 2021); [DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records \(CARIER\) System of Records](#), 81 FR 72080 (October 19, 2016); and [DHS/ICE-009 External Investigations](#), 85 FR 74362 (November 20, 2020). All CBP and ICE SORNs are available at: <https://www.dhs.gov/system-records-notice-sorns>.



Further, DHS stores forms and supplemental documentation in the A-File and processes applications and petitions in the respective DHS/USCIS case management system. Physical applications and supplemental documentation are stored in the physical (paper) A-File. Digital applications and supplemental documentation are stored in the electronic A-File maintained in an IT system. Depending on the underlying NARA retention schedule, the A-File records are held for a specific period of time, typically 100 years following the individual's date of birth, and then will be destroyed. A-files having a permanent retention schedule are not destroyed but are transferred 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.

PCIS is not subject to Paperwork Reduction Act requirements because PCIS does not collect information directly from an individual, and there are no forms associated with this collection. PCIS only collects information from other agency systems where case information and data was previously collected from USCIS immigration benefit request forms covered by the Paperwork Reduction Act. More information on these forms and the information source systems that may be subject to the Paperwork Reduction Act can be found in the applicable source system PIAs.

Section 2.0 Characterization of the Information

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

PCIS is a USCIS-wide initiative to improve how USCIS, ICE, and CBP users of the A-File handle, store, and leverage person data throughout USCIS, ICE, and CBP operations. PCIS retrieves, caches, and consolidates information from existing source system repositories on applicants, petitioners/sponsors, beneficiaries, attorneys, legal representatives, and individuals suspected of violating the immigration laws of the United States. PCIS employs existing historical and identity data declared on benefit requests, immigration encounters, and collected from enforcement actions to perform its functions. The comprehensive person-centric data is stored in an Identity Index, which contains an individual's immigration history, status, and biographic and biometric identity information.

Identity data is aggregated from other USCIS source systems, some of which are case management systems, as well as ICE and CBP law enforcement systems, and stored in the Identity Index. The Identity Index is the core of PCIS, enhancing the person-centric view to USCIS' historically transaction-based processes and data, as well as ICE and CBP law enforcement actions.



The Identity Index will require further development and technical integration with other existing systems, but it will not include additional data beyond that which is already collected by USCIS, ICE, and CBP for a benefit request or during an enforcement action. With PCIS envisioned to be the centralized, authoritative source of identity information, the Identity Index will serve as PCIS' data repository. The Identity Index was initially populated with all historical information from Enterprise Citizenship and Immigrations Services Centralized Operational Repository, a database information system. Currently, this database information system "data lake" contains data from the following source systems: Central Index System 2,⁷¹ Customer Profile Management System,⁷² USCIS Electronic Immigration System,⁷³ Computer Linked Application Information Management System 3,⁷⁴ Computer Linked Application Information Management System 4, Global,⁷⁵ Investor File Adjudication Case Tracker,⁷⁶ the Case and Activity Management for International Operations,⁷⁷ STACKS,⁷⁸ Consular Consolidated Database and RAILS⁷⁹ The Identity Index will also receive and share identity information with CBP's e3,⁸⁰ Unified Secondary,⁸¹ and Unified Immigration Portal⁸² systems, as well as ICE systems currently feeding USCIS Central Index System 2 system.

Below are the key data elements maintained within PCIS from other existing USCIS systems:

- First name;
- Middle name;
- Last name;
- Date of birth;
- Country of birth;
- Country of citizenship;

⁷¹ See Supra Note 14.

⁷² See Supra Note 15.

⁷³ See Supra Note 16.

⁷⁴ See Supra Note 17.

⁷⁵ See Supra Note 18.

⁷⁶ See Supra Note 19.

⁷⁷ See Supra Note 20.

⁷⁸ See Supra Note 21.

⁷⁹ See Supra Note 46.

⁸⁰ See Supra Note 24.

⁸¹ See Supra Note 25

⁸² See U.S. DEPARTMENT OF HOMELAND SECURITY, CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE UNIFIED IMMIGRATION PORTAL (UIP), DHS/CBP/PIA-072 (2022), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.



- Primary A-Number/other associated A-Numbers;
- Receipt number;
- Hair color;
- Eye color;
- Gender;
- Ethnicity;
- Race;
- Alias first names;
- Alias last names;
- Height;
- Weight;
- Parent names;
- Driver's License number;
- Fingerprint Identification Number;
- Class of Admission;
- I-94 Arrival/departure record number;
- Date Of Entry;
- Port Of Entry;
- Student & Exchange Visitor Information System number;
- USCIS Online Account number;
- Form type (form number);
- Employment Authorization Document number;
- Citizenship/Naturalization Certificate number;
- Certificate of Loss of Nationality;
- Photo image (when available);
- Passport number;
- Social Security number;



- Travel Document number;
- Visa Control number;
- Visa number;
- Currency/Monetary Instrument Report information;
- Current Address (residential and mailing);
- Historical address (residential and mailing);
- Email address;
- Telephone numbers (daytime and mobile);
- IDENT Encounter ID;
- Petitioner/sponsor name and contact information;
- Legal representative name and contact information;
- Familial relationships (declared and verified);
- DOJ Executive Office for Immigration Review Case Type and Decision;
- Non-immigrant ID;
- Education information;
- Occupation/employment information;
- FBI Universal Control Number;
- Physical characteristics;
- Removal history;
- Criminal history; and
- Family history.

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

The PCIS Initiative uses information maintained in USCIS source systems, DHS component systems, and external agency source systems. Specific data elements and the source system they are retrieved from are stated above in Section 2.1.

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.

Currently, an individual's data may be contained within many different databases, including case management and enforcement systems. Due to variations in the declaration and manual capture of biographic data, the data may not be successfully associated to the correct individual. PCIS seeks to address this inconsistency by providing a single point of collection for all data on a given individual. Then, through the data analytics process, an aggregated set of data for any given individual is created. Aggregated person data improves data quality by highlighting inconsistencies among a variety of USCIS source systems that store data on the same identity. PCIS is then able to automatically flag inconsistencies within the identity profile to ensure end users are aware additional analysis may be needed. Users can then take appropriate action to address the data inconsistency and/or association to a specific identity and make improved decisions as a result. Services built upon the PCIS Identity Index can be used to address future data issues by eliminating duplicate A-Numbers and indexing reliable person records for advanced search capabilities to reduce manual resolution of inconsistencies. This reduces the need for multiple connections across multiple data systems and ensures that all data pertaining to an individual is linked to that same individual.

PCIS collects the information directly from the source systems, which contain data typically collected directly from the individual applying for an immigration benefit or used by USCIS. PCIS also receives updates from the source systems on a regular basis. Immigration data is refreshed at least daily, with some data more frequently updated, depending on the source system. This updated information includes any changes made to the data as a result of the adjudication or enforcement process. The source systems' PIAs detail the opportunities USCIS customers and those subject to ICE and CBP enforcement have to correct their personally identifiable information.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the enhanced algorithms applied by PCIS microservices result in erroneous identity validations.

Mitigation: This risk is partially mitigated. USCIS uses the A-Number validation process to automatically compare biographic information against data in existing USCIS source systems. The A-Number Validation microservice uses the fuzzy match logic, a strong algorithm, to determine a match confidence level from the immigration benefit request form and the information the A-Number Validation microservice receives from USCIS source systems. Fuzzy match logic



can handle problems with imprecise and incomplete data, and it can model nonlinear functions of arbitrary complexity. By applying the fuzzy match logic, USCIS' goal is to improve record matching and reduce the total number of cases sent to manual resolution. If the confidence score meets or exceeds established thresholds, the A-Number Validation microservice returns a success message and the case continues processing with no manual intervention. Submissions that do not meet the match confidence threshold are queued in the USCIS case management for manual review to resolve the issue. The manual resolution process and redress procedures are further described in the respective system PIAs. USCIS tested the efficacy of this microservice by running the A-Number Validation microservice in parallel with the previous A-number validation process that occurred in the USCIS case management system. The testing results revealed there were no false positives, giving USCIS the confidence to solely rely on the A-Number Validation microservice. For mitigation of risk associated with its use of PCIS data after enhanced algorithms are applied, *see* section 3.4 below.

Privacy Risk: There is a risk that information in PCIS is replicated from multiple USCIS source systems and therefore may be inaccurate.

Mitigation: This risk is partially mitigated. PCIS extracts data from numerous USCIS source systems and loads the data elements into a coherent person-centric data structure that can be queried through a single system rather than requiring singular access to each system. USCIS adjudicators rely on the availability of the source systems to perform administrative and adjudicative tasks. Querying each system individually adversely impacts system availability and may cause considerable mission disruption such as decreased functionality and system lag times.

One of the main goals of PCIS is to improve the overall interoperability of USCIS systems. PCIS retrieves and uploads data from USCIS source systems on a near real-time basis. To mitigate the risk of inaccurate data within PCIS, the microservices frequently refresh data from USCIS source systems. Furthermore, the A-Number Validation microservice prevents the issuance of multiple A-Numbers which helps to prevent the promulgation of more inaccurate USCIS system data.

Privacy Risk: There is a privacy risk that an individual may be issued more than one A-Number resulting in multiple and duplicative records.

Mitigation: This risk is mitigated. PCIS was developed to associate all transactions and records to a person without using a specific identifier for a person such as an A-Number. Therefore, PCIS is mitigating the risk by auto-associating transactions together to form an identity where multiple A#s have been issued. PCIS clearly shows if a person has multiple A-Numbers through a banner on the user interface and also lists each A-Number with a tag of Primary, Secondary, Associated, or Unconsolidated. At the time the immigration record is needed for use, PCIS will indicate a person has multiple A-Numbers, at which point USCIS will consolidate all accurately

associated A-Numbers and identify the primary and secondary A-Numbers per the USCIS Records Policy Manual.⁸³ A primary A-Number is the number currently assigned to the existing physical paper file. Secondary A-Numbers are those that have been consolidated into the primary A-Number.

To further mitigate the risk moving forward, USCIS developed the PCIS A-Number Management Services which perform validation on an individual to determine if an A-Number has already been assigned prior to issuing a new A-Number. This service is being integrated with systems responsible for issuing A-Numbers to centralize the process to prevent duplicate A-Numbers from being issued to the same person.

Privacy Risk: There is a risk the data that the PCIS Identity Index receives is inaccurate.

Mitigation: This risk is partially mitigated. The PCIS Identity Index depends on the accuracy and quality of information provided by the source systems. Data maintained in the Identity Index is updated at least daily, and in some case more frequently, to capture data changes within the source systems. This process reduces the risk of data discrepancies between the Identity Index and the source systems. In addition, the Identity Index access is limited to read-only connectivity, to preserve the integrity and accuracy of the information derived from USCIS, ICE, and CBP systems.

For each of the source systems, USCIS relies on the accuracy of the information provided by the individual during an encounter with ICE or CBP or by an immigration benefit requestor and/or legal representatives.

When submitting an immigration benefit request to USCIS, requestors must certify on the respective forms that the information submitted is complete, true, and correct. USCIS presumes the information submitted is accurate and verifies the information against multiple sources during the review process. USCIS also gives individuals opportunities during and after the completion of the immigration benefit request process to correct information provided or received and to respond to any adverse information received from external sources in accordance with current law, regulations, and policies. Furthermore, biometrics are submitted for most major immigration benefit requests and law enforcement actions, providing further assurances that the biographic information and associated immigration record are correct.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

PCIS supports the USCIS mission of administering and adjudicating immigration benefit

⁸³ The USCIS Records Policy Manual is an internal USCIS document and serves as the official policy governing immigration information management at the Agency.



requests and other services requiring the use of immigration data. Eventually, PCIS will also help support ICE, CBP, and other DHS component missions by providing a comprehensive view of an individual's immigration history and filings for benefit requests with USCIS. USCIS plans to use these to establish a person-centric data service by consolidating information about individuals into one central user interface. Uses of PCIS include, but are not limited to:

- Associating USCIS, DHS, and external source systems data in a person-centric manner;
- Linking the A-Number and USCIS Online Account Number issuance process to biometrics; and
- Managing the identity resolution process.

Through PCIS, USCIS creates a single, trusted source of biographical and biometric information to holistically link all elements of these data points and maintain them in a single authoritative source. PCIS includes data, and user functionality from Central Index System 2, Person Centric Query Service, and also include person data from USCIS systems (e.g., USCIS Electronic Immigration System, Computer Linked Application Information Management System 3, Computer Linked Application Information Management System 4, Global, Investor File Adjudication Case Tracker, and Case and Activity Management for International Operations), as well as integration with the Customer Profile Management System. The comprehensive person data is stored in an Identity Index, which contains an individual's immigration history, status, and biographic and biometric identity information.

As part of DHS support for Operation Allies Welcome,⁸⁴ PCIS shares person data with DHS' Hummingbird system.⁸⁵ Hummingbird was formerly owned and operated by the Department of State and contains information pertaining to Operation Allies Welcome participants, generated by multiple agencies who utilized the system to centralize certain information, including medical examination/vaccination, and immigration paperwork for refugee applicants before their resettlement in the United States. PCIS pushes Central Index System 2 data to Hummingbird when an individual's A-file is created and updates the Hummingbird record with key adjudication data to properly track the Operation Allies Welcome population through the biometrics submission and employment authorization process.

The PCIS interface allows users to search using an elastic search methodology with a variety of data elements stored in the Identity Index (e.g., A-number, Fingerprint Identification

⁸⁴ An operation where multiple federal agencies, including Department of Defense, DOS, Health and Human Services, have come together to welcome vulnerable Afghans, including those who worked alongside the U.S. in Afghanistan for the past two decades, to the United States and assist them to safely resettle in the U.S.

⁸⁵ See U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR HUMMINGBIRD, DHS/ALL/PIA-093 (2022), available at <https://www.dhs.gov/privacy-documents-department-wide-programs>.



Number, first name, last name, date of birth). The enhanced search functions display both exact results and similar results based on search criteria to empower users to find the desired individual or narrow down the search as needed. Search results include high level, relevant individual information for users to rely on with confidence, saving search time in further researching the result. Each result leads to a single profile that serves as a one-stop shop to view biographic and biometric information associated with the individual's identity, history of encounters with DHS components, immigration status, history of immigration benefits, and immigration benefit outcomes. Additionally, users can drill down to see details of encounters and adjudications.

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. PCIS only permits information searches regarding a specific individual and the consolidation of that individual's information. PCIS is not used to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly.

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

Yes, USCIS, CBP, and ICE users currently use information contained in PCIS through the PCIS User Interface. USCIS maintains controls over access to PCIS to ensure only those with proper authority and mission need are allowed to have direct access. Additionally, USCIS has a formal review and approval process for new sharing agreements. Any new use of information or new system access requests must go through the formal information request process and be approved by the proper authorities at USCIS (e.g., USCIS Chief Privacy Officer, Chief Information Security Officer, Office of the Chief Data Officer, Office of Chief Counsel, and the respective Program Offices) and, as necessary, their respective counterparts at DHS Headquarters prior to implementation. PCIS system access would only be provided to users pursuant to the SORNs governing the data, and consistent with information-sharing access agreements and applicable laws, regulations, and policies. The USCIS governance process will develop roles for external users, for both access to PCIS information and the PCIS User Interface, as appropriate.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that the PCIS Identity Index may associate a record with the incorrect applicant.

Mitigation: This risk is partially mitigated. The PCIS Identity Index mitigates this risk by



using a strong matching algorithm, which includes matching an A-Number along with first name, last name, date of birth, country of birth, Fingerprint Identification Number, Social Security number, and other attributes to tie together records pertaining to a single individual. The PCIS Identity Index also provides a comparison view that allows the user to view the person-centric data from each of the underlying systems and determine whether an incorrect match was rendered due to incorrect data stored in the connected IT systems. For individuals who believe they have been adversely affected by incorrect association of PCIS information based on USCIS, ICE, or CBP records, the individual should follow the procedures specified in Section 7.1 below. USCIS, ICE, and CBP will coordinate during the redress and correction process to ensure any necessary corrections are made to the appropriate records. The risk is further mitigated through the Identity Resolution Queue which allows a human-in-the-loop to make necessary corrections to ensure the integrity of the identity index.

Section 4.0 Notice

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

PCIS does not collect information directly from individuals. However, USCIS is providing notice about this system through this PIA. Each DHS source system provides notice through a PIA and SORN, which are available on the public facing DHS Privacy Office website.

Furthermore, USCIS provides multiple forms of notice to immigration benefit requestors when the information is originally collected. Each immigration benefit request, regardless of whether it is paper or electronic undergoes a PRA review often requiring public comment periods before implementation. Each form also contains a required Privacy Notice detailing USCIS' 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, immigration benefit requestors receive general notice through this PIA, the respective USCIS source system PIAs, and the associated SORNs (DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking SORN,⁸⁶ DHS/USCIS-007 Benefits Information System SORN,⁸⁷ DHS/USCIS-010 Asylum Information Prescreening SORN,⁸⁸ DHS/USCIS-017 Refugee Case Processing and Security Screening Information SORN,⁸⁹ DHS/USCIS-018 Immigration Biometric

⁸⁶ See Supra Note 64.

⁸⁷ See Supra Note 65.

⁸⁸ See Supra Note 66.

⁸⁹ See Supra Note 67.



and Background Check SORN,⁹⁰ and DHS/USCIS-005 Inter-Country Adoptions Security SORN).⁹¹

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

As part of the immigration benefit request process, individuals consent to USCIS' overall use of the information submitted for adjudication purposes. Individuals who apply for immigration benefits have an opportunity and ability to decline to provide information. USCIS immigration forms require the individual to provide biographic and/or biometric information, which is critical to making an informed adjudication decision. Thus, failure to submit such information may impede USCIS processing and properly adjudicating the immigration benefit request and thus may preclude the applicant from receiving the immigration benefit requested.

CBP and ICE typically do not offer individuals an opportunity to decline to provide or use their information, due to the circumstances of encounters and purpose for collecting the information—immigration and law enforcement.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Because PCIS does not directly collect information from an individual and relies on other USCIS, ICE, and CBP source systems for information, there is a risk individuals will not receive notice of the purpose for which the PCIS Identity Index uses their information.

Mitigation: This risk is partially mitigated. This PIA serves as notice to the public regarding the PCIS Initiative and the PCIS Identity Index. USCIS, ICE, and CBP provide the individual with a Privacy Notice explaining the purpose of collection at the original point of collection. Each immigration benefit request form contains a Privacy Notice detailing USCIS, ICE, or CBP'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, ICE, or CBP. Furthermore, notice of the source systems interaction with PCIS is provided with this PIA and will be further provided through updates to the applicable source system PIAs and the applicable SORNs.

Section 5.0 Data Retention by the project

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

PCIS retrieves data from existing USCIS, ICE, and CBP source systems for inclusion in the Identity Index. To create this single person-centric view of individuals, PCIS includes data, and user functionality from Central Index System 2, Person Centric Query Service, and also

⁹⁰ See Supra Note 68.

⁹¹ See Supra Note 69.



includes person data from USCIS systems (e.g., case management systems) as well as integration with the Customer Profile Management System. The Identity Index is configured to have the ability to retain data elements based on the retention guidelines of the source system.

USCIS and NARA negotiated the disposition schedules for the source systems to ensure that USCIS retains data for the minimum time needed to process the immigration benefit request and availability for other decision-making processes. NARA approved the Central Index System 2 retention schedule N1-566-10-01 on November 05, 2009. According to this retention schedule, Central Index System 2 records are permanent and USCIS will transfer A-Files to the custody of NARA 100 years after the individual's date of birth. Furthermore, Customer Profile Management System data will be retained for 100 years from the individual's date of birth in accordance with NARA Disposition Authority Number DAA 0563-2013-0001-0005.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk PCIS may maintain information for a period longer than necessary to achieve agency objectives.

Mitigation: This risk is mitigated. USCIS mitigates this risk by following the National Archives and Records Administration-approved retention schedule for each source system's data. The NARA proposed and approved schedules for each source system match the requirements of the Federal Records Act and the stated purpose and mission of the system. The Identity Index is configured to have the ability to retain data elements based on the retention guidelines of the source system. USCIS and NARA carefully negotiated the disposition schedules for the source systems to ensure that USCIS retains data for the minimum time needed to process the immigration benefit request and availability for other decision-making processes.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS a 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.

PCIS does not share data outside of DHS as part of its normal operations. Any future, external PCIS system access requests would undergo the proper vetting, authorization, and data sharing agreement requirements in accordance with USCIS and DHS policies and regulations. In addition, USCIS will amend this PIA to consider risks associated with any sharing of information outside of DHS.

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



PCIS external sharing parameters are within the same scope as the SORNs noted in 1.2.

6.3 Does the project place limitations on re-dissemination?

As mentioned, PCIS does not share data outside of DHS as part of its normal operations. However, any future data sharing agreements with external agencies/organizations would include the required limitations on re-dissemination (including third-party disclosure, protected information, etc.).

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

PCIS does not share A-File data outside of DHS as part of its normal agency operations. Any future data sharing agreements will be negotiated and executed in accordance with USCIS and DHS policies and regulations. The system also creates a log of information accessed by users, and can be used to determine what information was accessed and by whom.

Section 7.0 Redress

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

Individuals seeking access to their information held by USCIS, ICE, or CBP may gain access to their records by filing a Privacy Act request if they are a U.S. citizen or Lawful Permanent Resident or if they are a citizen of a country covered by the Judicial Redress Act. Individuals not covered by the Privacy Act or Judicial Redress Act still may obtain access to records consistent with agency policy⁹² and/or FOIA unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. Any individual seeking access to their information should direct their request to one of the following addresses:

USCIS National Records Center (NRC)
FOIA/PA Office
P.O. Box 648010
Lee's Summit, MO 64064-8010

ICE FOIA/PA Headquarters Office
500 12th Street SW, Stop 5009
Washington, D.C. 20536-5009

⁹² See DHS Privacy Policy Regarding the Collection, Use, Retention, and Dissemination of Personally Identifiable Information, 2022 available at https://www.dhs.gov/sites/default/files/2022-05/mgmt-dir_262-16-00-privacy-policy-regarding-collection-use-retention-dissemination-pii.pdf.



U.S. Customs and Border Protection (CBP)⁹³
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, D.C. 20229
Fax Number: (202) 325-1476

Persons not covered by the Privacy Act or Judicial Redress Act are not able to amend their records through FOIA. Should a non-citizen find inaccurate information in their record received through FOIA, they may visit a local USCIS Field Office to identify and amend inaccurate records with evidence. Further information for Privacy Act and FOIA requests for USCIS records can also be found 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, lawful permanent residents, and individuals covered by the Judicial Redress Act are afforded the ability to correct information by filing a Privacy Act Amendment as discussed in Section 7.1. U.S. citizens, lawful permanent residents, and persons covered by the Judicial Redress Act should submit requests to contest or amend information contained in USCIS systems to the USCIS FOIA/Privacy Act Office. 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 their record received through FOIA, they 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 about the procedures for correcting their information through this PIA, source system SORNs and PIAs, Privacy Notices, and through the USCIS website. Specifically, the SORNs set forth in Section 1.2 provide individuals with guidance regarding the procedures for correcting information. The Privacy Notices, including notice of an individual's right to correct information, are also contained in the instructions to all immigration forms published by USCIS.

7.4 Privacy Impact Analysis: Related to Redress

⁹³ Individuals seeking notification of and access to information contained in CBP records may gain access to certain information by filing a Freedom of Information Act (FOIA) request with CBP at <https://foia.cbp.gov/>.



There are no risks associated with redress in relation to the Person Centric Service Microservices or the PCIS Initiative. USCIS provides individuals access to appropriate records when requested and approved through a FOIA/Privacy Act request.

Section 8.0 Auditing and Accountability

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

USCIS ensures that the practices stated in this PIA are followed by leveraging training, policies, rules of behavior, and auditing and accountability. USCIS established access and security controls to mitigate privacy risks associated with authorized and unauthorized uses, namely misuse and inappropriate dissemination of data. DHS security specifications require auditing capabilities that log the transactions of users in order to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. All USCIS systems employ auditing measures and technical safeguards to prevent the misuse of data. Auditing will be managed by the systems using the Person Centric Service microservices.

USCIS follows DHS policy and requirements for information assurance and security for PCIS. All PCIS Initiatives undergo the DHS system security authorization process to ensure DHS standards for security policy, guidance, and architecture requirements are met before any source data is duplicated into the system. Through the system security authorization process, USCIS evaluates each system to determine which set of robust security controls are to be implemented in order to safeguard the confidentiality, integrity, and availability of the information residing in the system.

USCIS is required to ensure appropriate technical, administrative, and physical controls are properly implemented to meet DHS system security policy requirements and safeguard the information. USCIS employs technical and security controls to preserve the confidentiality, integrity, and availability of the data, which are validated during the security authorization process. These technical and security controls mitigate the privacy risks associated with unauthorized access and disclosure. Security measures are in place to ensure that the personally identifiable information in PCIS is accessed and used in accordance with DHS and USCIS policies and guidelines.

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

All USCIS, ICE, and CBP employees and contractors are required to complete annual privacy and computer security awareness training to ensure their understanding of proper handling and securing of personally identifiable information. Privacy training addresses appropriate privacy



concerns, including Privacy Act obligations (e.g., SORNs, Privacy Act Statements/Notices). The Computer Security Awareness Training examines appropriate technical, physical, and administrative control measures to safeguard information. In addition, Quality Assurance Reviewers attend quality assurance calibration sessions. The USCIS, ICE, and CBP Offices of Privacy maintains a record of certificates of training on all employees and contractors.

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

PCIS is comprised of back-end services that are integrated into USCIS interconnected systems to enhance the systems respective functionality. USCIS only grants back-end access to authorized personnel on a strictly need-to-know basis. User access to the interconnected systems is discussed in the relevant USCIS, ICE, or CBP system or program PIAs. USCIS audits user access in accordance with the DHS Sensitive Systems Policy Directive 4300A, which requires auditing capabilities that log the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify information by user identification, network terminal identification, date, time, and data accessed. All USCIS, ICE, and CBP systems employ auditing measures and technical safeguards to prevent the misuse of data. USCIS will perform ongoing evaluations to ensure the effectiveness of the security procedures and safeguards implemented.

Access privileges are limited by establishing role-based user accounts to minimize access to information that the user does not need to perform essential job functions. The employee's current job functions determine their need-to-know. The employee's supervisor must validate that the employee needs access to the information. Moreover, USCIS limits users' access privileges by ensuring they have authorized logon credentials (i.e., DHS-issued user ID and password) and have an established role-based user account.

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, such as DHS Headquarters (including the Office of General Counsel, the Office for Civil Rights and Civil Liberties, the Office of Intelligence and Analysis, and the Privacy Office), USCIS Privacy Officer, Chief of Information Security Officer, Office of the Chief Counsel, and the respective Program Office.



Responsible Official

Angela Washington
USCIS Chief Privacy Officer
U.S. Citizenship and Immigration Services
U.S. Department of Homeland Security
(240) 721-3701

Approval Signature

Original, signed copy on file at the DHS Privacy Office.

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717