Privacy Impact Assessment
for the

International Case Tracking System (ICTS)

DHS/USCIS/PIA-069

February 2, 2018

Contact Point
Donald K. Hawkins
Office of Privacy
U.S. Citizenship and Immigration Services
202-272-8030

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The U.S. Government has entered into information sharing agreements with international partners for the exchange of information to support border security, lawful immigration, and other DHS missions. The U.S. Citizenship and Immigration Services (USCIS) National Records Center (NRC) is responsible for responding to information requests from foreign partners when information sharing agreements and appropriate waivers are in place as part of the International Information Sharing (IIS) Program. To streamline the intake of secondary international information requests, USCIS NRC developed the International Case Tracking System (ICTS). USCIS is updating this PIA on February 2, 2018, to account for incoming secondary follow up requests from New Zealand. At this time, USCIS is only receiving and responding to secondary queries from New Zealand, Canada, and Australia. USCIS is conducting this privacy impact assessment (PIA) to cover the receipt, creation, tracking, and processing of cases as part of the international data sharing efforts. USCIS will update this PIA as USCIS engages with other foreign partners.

Overview

The U.S. Government has entered into information sharing agreements with international partners for the exchange of information to support border security, lawful immigration and other Department of Homeland Security (DHS) missions. The U.S. Citizenship and Immigration Services (USCIS) National Records Center (NRC) is responsible for responding to secondary requests from foreign partners, under the terms of the information sharing agreements that USCIS NRC has determined cover immigration vetting. An initial match against a fingerprint maintained in the DHS National Protection and Programs Directorate's (NPPD) Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT) may reveal that the subject of the query has been previously encountered by USCIS, and the foreign partner may affirmatively request information from USCIS beyond the limited biographic information held in IDENT.[1]

DHS currently shares information with members of "the Five Country Conference" (FCC)[2] under Visa and Immigration Information Agreements. The purpose of the Visa and Immigration Information Agreements is to support immigration processes, including asylum, visa, and refugee determinations, as well as admissibility, among the FCC partners.[3]

---

[1] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy.

[2] The Five Country Conference (FCC) is a forum for cooperation on migration and border security between the countries of Australia, Canada, New Zealand, the United Kingdom, and the United States (collectively called the FCC partners).

[3] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) Appendix B, *available at* www.dhs.gov/privacy.

The NPPD OBIM, through IDENT, supports the initial query and response process for international biometric sharing on behalf of DHS. IDENT serves as a biographic and biometric repository for the Department. IDENT stores and processes biometric data from DHS components and other providers — including digital fingerprints, photographs, iris scans, and facial images— and links biometrics with limited biographic information to establish and verify identities in support of the DHS mission.

As part of the benefit adjudication process, USCIS collects biometric and associated biographic information and stores it in Customer Profile Management System (CPMS).[4] USCIS sends fingerprints, photograph, and limited biographic information from CPMS to IDENT. IDENT assigns a unique identifier (Fingerprint Identification Number (FIN)) to an individual's biometric the first time the individual is encountered. This unique enumerator or FIN is returned to CPMS.

Under international agreements and appropriate waivers,[5] foreign partners are able search individual fingerprint records and associated biographic data maintained by DHS. As part of this process, IDENT receives biometric and associated data from foreign partner operating systems and automatically compares those records against biometrics contained in IDENT. If there is a match to an existing biometric record in IDENT, IDENT acknowledges the match and shares limited biographic elements associated to the biometric to the foreign partner. If there is no match on a biometric query, or if there is a match to a record that is protected under special confidentiality provisions of the law, IDENT returns a "no match" response to the foreign partner operating system.

In the event there is a "match," the foreign partner may request additional information relating to the matched individual from the source system. If the source system is maintained by USCIS, foreign partners may request additional information via IDENT to receive the most up-to-date information from USCIS. This information is to be used by the foreign partner to assist with adjudicative or enforcement-related decisions on those submitting asylum, refugee, and visa applications or when the individual is suspected or convicted of a serious crime. The information provided by USCIS may be used to confirm the identity of an applicant, class of admission, and current immigration status. It may also assist the foreign partner with investigating known terrorism ties or suspected ties with terrorism, and with identifying potential fraud or other crimes. At this time, USCIS is only receiving and responding to secondary queries from New Zealand, Canada, and Australia.

[4] *See* DHS/USCIS/PIA-060 Customer Profile Management Service (CPMS), *available at* www.dhs.gov/privacy.
[5] The federal regulation at 8 CFR 208.6 generally prohibits the disclosure to third parties of information contained in or pertaining to asylum applications, credible fear determinations, and reasonable fear determination absent the applicant's signed written consent or the written authorization of the Secretary of Homeland Security.

Incoming Follow-Up Requests

Foreign partners (i.e., New Zealand, Canada, and Australia) may send secondary information requests through IDENT for additional information. As the DHS repository of biometric data, information maintained by IDENT is collected by DHS components, including USCIS. If the source system is a system maintained by USCIS, foreign partners may request additional information via IDENT to receive the most up-to-date information from USCIS. IDENT, serving as an interface, sends the secondary request to USCIS Customer Profile Management System (CPMS).[6] CPMS then sends the foreign partner request to the International Case Tracking System (ICTS), which is managed by the USCIS NRC.

A typical transaction begins with USCIS analysts downloading foreign partner's requests from CPMS. As a carry-over from the existing manual process, each country uses its own unique information request template (herein thereafter referred to as country-specific request), which generally includes the subject's associated biographic information (such as IDENT FIN, Alien Number (A-Number), and full name), foreign partner Identification Number, and requested information and documentation. Each country-specific request template collects the same information but has slight formatting differences. USCIS is developing a uniform template for use with all foreign partners in order for ICTS to automatically ingest and create cases for each secondary request. USCIS uses ICTS to record the foreign partner request and replace the manual process for responding to requests for additional information.

Case Creation

Each incoming country-specific request is manually entered by USCIS analysts into ICTS to create a case for tracking purposes. Each case profile contains the following information:

Information about the record subject:

- A-Number;
- IDENT FIN;
- USCIS File type (i.e., A-File,[7] Temporary File,[8] Receipt File[9]) and location; and

[6] *See* DHS/USCIS/PIA-060 Customer Profile Management Service (CPMS), *available at* www.dhs.gov/privacy.
[7] USCIS A-Files may exist in paper, electronic, or hybrid (both electronic and paper) form. Electronic A-Files may exist both in Enterprise Document Management System (EDMS) and USCIS Electronic Immigration System (USCIS ELIS). *See* DHS/USCIS/PIA-003 Integrated Digitization Document Management Program (IDDMP), for information about EDMS and DHS/USCIS/PIA-056 USCIS Electronic Immigration System (USCIS ELIS), *available at* www.dhs.gov/privacy.
[8] Temporary Files (T-Files) are temporary files that are created to store permanent documentation when the original A-File cannot immediately be located, or is pending receipt from another USCIS Office.
[9] Receipt Files serve as an adjunct to the A-File. Each Receipt File houses a specific form type including supporting documentation, and each form type and/or group of form types must be maintained for various time periods based on the administrative, fiscal, and legal needs of USCIS.

- Information and supporting documentation about the record subject being requested by the Foreign Partner (e.g., current immigration status, application/petition history and decisions, prior immigration violations, and biographic information.

Information about the country requestor is:

- Country; and
- Unique Country-specific Tracking Number.

Information about the USCIS Employee:

- USCIS Analyst User Name; and
- Date/Time of request creation.

Once a case is created, ICTS generates a working ticket with a system generated tracking number. The USCIS analysts use National File Tracking System (NFTS)[10] to determine the file location. A pull ticket is created and printed for files located at the National Records Center (NRC) and Federal Records Center (FRC) to initiate a manual retrieval of the A-File or other related files. The physical working ticket is then placed in queue for a USCIS contractor to retrieve the A-File for the USCIS analyst to process. Each printed request accompanies the A-File. Digitized files and externally-located files are tracked electronically through ICTS reporting functions. USCIS analyst also record and track case processing data (date and time) and case status in ICTS.

Responding to Information Requests

Depending on the requested information, USCIS analysts review the paper or electronic A-File to validate the identity of the individual. USCIS analysts also review the A-File to determine which DHS component the individual had previously interacted with to include interaction with USCIS or other DHS Components, such as U.S. Immigration and Customs Enforcement (ICE) or U.S. Customs and Border Protection (CBP), which also contribute to and manage A-File content. USCIS analysts may scan requested documents from the A-File and temporarily store the documents in a secured shared drive.

USCIS analyst may consult with other USCIS, DHS, and external systems to create a consolidated response for the foreign partner:

USCIS Systems

- **Central Index System (CIS)** is a repository of electronic data that summarizes the history of an immigrant**.** CIS contains information on the status of individuals, including lawful permanent residents, naturalized citizens, U.S. border crossers,

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

apprehended aliens, legalized aliens, aliens who have been issued employment authorizations, and other individuals of interest to DHS.[11]

- **USCIS Electronic Information System (USCIS ELIS)** is an electronic case management system that allows USCIS to process certain immigration benefit requests.[12]
- **Computer Linked Application Information Management System (CLAIMS 3)** manages the adjudication process for most domestically-filed, paper-based, immigration benefit filings with the exception of naturalization, intercountry adoption, and certain requests for asylum and refugee status.[13]
- **Person Centric Query System (PCQS)** allows users to submit a single query and view all transactions involving an immigrant or nonimmigrant across multiple DHS and external systems.[14]

DHS Component Systems

- **ICE Enforcement Alien Removal Module (EARM)** is an application that supports ICE's processing and removal of aliens from the United States. ICE uses EARM primarily as a case management tool to track the status of alien removal proceedings.[15]

External Agency Systems

- **Department of State (DOS) Worldwide Refugee Admissions Processing System (WRAPS)** tracks refugee applicants as they move through the required refugee processing steps until arrival in the United States.[16]

During this process, the USCIS analyst updates ICTS with any special information about the file (File retired, protected status of the alien, digitized file, etc.).

To formally respond back to the information request, the USCIS analyst uses the country-specific request template to provide a synopsis of the information in a text box. In addition to the country-specific request template, USCIS may also provide scanned documents such as

[11] *See* DHS/USCIS/PIA-009 Central Index System (CIS), *available at* www.dhs.gov/privacy.
[12] *See* DHS/USCIS/PIA-056 USCIS Electronic Immigration System (USCIS ELIS), *available at* www.dhs.gov/privacy.
[13] *See* DHS/USCIS/PIA-016(a) Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems, *available at* www.dhs.gov/privacy.
[14] *See* DHS/USCIS/PIA-010 Person Centric Query Service, *available at* www.dhs.gov/privacy.
[15] *See* DHS/ICE-PIA-015(b) Enforcement Integrated Database (EID) ENFORCE Alien Removal Module (EARM 3.0), *available at* www.dhs.gov/privacy.
[16] WRAPS is the DOS case management database used for all refugee applicants processed for resettlement consideration to the United States. Please see the DOS WRAPS PIA and SORN for more information on this system and the information it collects, uses, and maintains, *available at* https://2001-2009.state.gov/documents/organization/101146.pdf.

applications, photographs, and fingerprints. All scanned documents are appropriately redacted. Redactions occur for Social Security numbers (SSN) and third party names (i.e., children, spouse, parents). The USCIS analyst uploads the country-specific request and scanned documents from the shared drive to ICTS and the package is electronically transmitted to CPMS. CPMS then acts as a pass-through to IDENT, in which IDENT sends the package to the foreign partner operating system.

The scanned documentation is not retained in ICTS. The scanned documentation is stored in CPMS in accordance with the NARA approved schedule [NARA Disposition Authority Number DAA-0563-2013-0001-0005]. Once ICTS transmits information to IDENT, a copy of the attached documents is stored on the secured USCIS NRC shared drive (on the USCIS local area network) for one week only. The shared drive has privacy and security safeguards to only allow USCIS staff who have permission to access the documentation. ICTS only retains the created case profile and the information/documentation that was released in response to the foreign partner request.

Reporting

Information contained in ICTS is used to generate a number of statistical reports to measure and evaluate workload for proper resource allocation. ICTS data is used to generate reports to identify pending cases, to measure productivity trends, and to calculate average case processing times. USCIS also generates granular level reports to identify status of cases assigned to a particular USCIS analyst, which allows supervisors to identify the oldest cases in queue for processing.

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?

Immigration and Nationality Act, 8 U.S.C. §§ 1103, 1158, 1225, and 1228. At this time, USCIS is only receiving and responding to secondary queries from New Zealand, Canada, and Australia. DHS has bilateral international information sharing agreements and memoranda of understanding (MOU) between DHS and its foreign partners under which USCIS information may be shared.[17] [18]

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

[17] A full list of current DHS Agreements with the Five Country Conference Partners may be found in Appendix A.
[18] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) Appendices for Canada and Australia, *available at* www.dhs.gov/privacy.

The collection, use, maintenance, and dissemination of information is collected in accordance with the following SORNs:

- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, which covers the collection, use, and dissemination of information from the A-File.[19]
- DHS/USCIS-002 Background Check Service, which covers the collection and use of biometric and associated biographic information for background check purposes.[20]
- DHS/USCIS-003 Biometric Storage System, which covers the storage and dissemination of biometric and associated biographic information.[21]
- DHS/USCIS-007 Benefit Information System, which covers the collection, use, and dissemination of information from CLAIMS 3, USCIS ELIS, and PCQS.[22]
- DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, which covers the collection, use, and dissemination of information about asylum applicants.[23]
- DHS/USCIS-017 Refugee Case Processing and Security Screening Information System of Records, which covers the collection, use, and dissemination of information about refugee applicants.[24]

In addition, the USCIS Office of Privacy is consolidating DHS/USCIS-002 Background Check Service and DHS/USCIS-003 Biometric Storage System SORNs into the Immigration Biometric and Background Check SORN to holistically cover biometric and biographic screening and background checks for USCIS customers and international partners.

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

Yes. ICTS falls under the Digital Innovation and Development – Information Technology (DID-IT) accreditation boundary. DID-IT completed the security assessment and authorization documentation in August 2013, and was accepted into the Ongoing Authorization program. Ongoing Authorization requires DID-IT, including ICTS, to be reviewed on a monthly basis and maintain its security posture to maintain its Authority to Operate.

---

[19] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sep. 18, 2017).
[20] DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007).
[21] DHS/USCIS-003 Biometric Storage System, 72 FR 17172 (April 3, 2007).
[22] DHS/USCIS-007 Benefit Information System, 81 FR 72069 (Oct. 19, 2016).
[23] DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (Nov. 30, 2015).
[24] DHS/USCIS-017 Refugee Case Processing and Security Screening Information System of Records, 81 FR 72075 (Oct. 19, 2016).

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

No. USCIS is working with NARA to develop a records retention schedule to cover ICTS records. USCIS proposes to delete and destroy the information six (6) years from the last completed action. The proposed retention will allow analysts to refer to historical records of past searches, alleviating the need to request the physical file if no material change has occurred.

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

Not applicable.

Section 2.0 Characterization of the Information

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

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

ICTS collects and maintains the following information:

Information about the record subject includes:

- A-Number;
- IDENT FIN;
- File type (i.e., A-File,[25] Temporary File,[26] Receipt File[27]) and location;
- Information and supporting documentation about the record subject being requested by the Foreign Partner (e.g., current immigration status, application/petition history and decisions, prior immigration violations, and biographic information); and
- USCIS's Response.

[25] USCIS A-Files may exist in paper, electronic, or hybrid (both electronic and paper) form. Electronic A-Files may exist both in EDMS and USCIS ELIS.
[26] Temporary Files (T-Files) are temporary files that are created to store permanent documentation when the original A-File cannot immediately be located, or is pending receipt from another USCIS Office.
[27] Receipt Files serve as an adjunct to the A-File. Each Receipt File houses a specific form type including supporting documentation, and each form type and/or group of form types must be maintained for various time periods based on the administrative, fiscal, and legal needs of USCIS.

Information about the country requestor includes:

- Country; and
- Unique Country-specific Tracking Number.

Information about the USCIS Employee includes:

- USCIS Analyst User Name; and
- Date/Time of action (i.e., received, printed, closed).

Information generated by ICTS to create a pull ticket include:

- Tracking Number.

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

The information contained in ICTS is collected from foreign partners who request additional information about individuals after information they have submitted results in a match to identity information contained in IDENT. USCIS analysts use USCIS systems, other DHS Components systems, and non-DHS systems to respond to follow-up information requests from foreign partners.

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

Not applicable.

2.4 Discuss how accuracy of the data is ensured.

USCIS analysts manually enter foreign partner requests into ICTS for case processing purposes. All USCIS personnel are provided with the opportunity to review and edit information prior to and after its submission for manually entered data. Through system coding, ICTS is configured to validate data entry to mitigate typological errors (e.g., the system rejects 00/00/00 birthdates). ICTS records are randomly reviewed for quality assurance purposes to ensure that records are created correctly and that all appropriate updates have been made when cases. USCIS analysts are able to correct and edit data inaccuracies at any stage of the process.

The information USCIS collects and transfers to the foreign partner is assumed to be accurate because it is collected directly from the benefit requestor. USCIS ensures data accuracy of its systems by collecting biographic and biometric information directly from the benefit requestor. USCIS biometrically verifies the accuracy of the information provided through the background check process. Biometric verification is an identity authentication process used to

confirm a claimed identity through uniquely identifiable biological traits. USCIS analysts cross references and use multiple USCIS, DHS, and non-DHS systems to respond to foreign partners to ensure the most accurate and complete information is shared with the foreign partner. USCIS analysts also uses the paper or electronic A-File as a source. USCIS analysts receive training on these procedures to maintain quality and consistency in processing and responding to foreign partner requests.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that inaccurate data is captured within ICTS because the country requests are manually entered into the system.

Mitigation: This risk is partially mitigated. To improve efficiency and mitigate the data quality risks, USCIS automated the email process by developing a system-to-system solution. In addition to improving data quality, the system to system solution is more secure than the use of emails, which could inadvertently be sent to an unauthorized person or potentially be intercepted during transmission. Moreover, the use of CPMS and ICTS allows USCIS to easily track, monitor, and report on international information sharing and accurately account for disclosures. The new automated process can handle a greater volume of queries, thus creating efficiencies required to obtain the necessary information about individuals in a timely manner.

DHS is also working to standardize the country-specific information request template to auto-populate the information in ICTS. Currently, each country uses its own country-specific request template to request for additional information. Each country-specific request template collects the same information but has slight formatting differences. Because of these variations, USCIS analysts are required to manually enter information into ICTS. USCIS configured ICTS through program coding to mitigate or prevent inconsistencies in data. The data fields in the input screen are configured to limit the possibility of entering malformed data (e.g., the system rejects 00/00/00 birthdates). Data entry personnel are provided with the opportunity to review and edit information prior to and after their submission. Additionally, authorized USCIS personnel have the ability to correct and edit inaccuracies, at any stage of the process, brought to their attention internally.

To establish and maintain quality and consistency in processing information requests, all supervisors must ensure that all employees under their supervision involved in the processing of information requests have been trained on these procedures. All Immigration Service Officers are required to take Immigration Services Officer Basic Training Program (BASIC) training which provide an overview their roles and responsibilities in adjudicating benefits applications and petitions. The BASIC curriculum covers public service, immigration law, customer service, fraud and national security, and privacy.

USCIS has quality assurance review and internal audits, in which individual case files are randomly selected and reviewed by a team of experienced analysts. Quality Assurance reviews are an integral part of the information sharing process. Reviewers use a checklist to assess and record the quality of each case. USCIS is working to automate the process and remove the opportunity for human error. Statistically valid data collections and effective analysis methods can be used to bring about process improvements and ensure that international sharing processing is consistent across all USCIS analysts.

Privacy Risk: There is a risk that the foreign partner may submit inaccurate information, which will then be recorded in ICTS.

Mitigation: This risk is partially mitigated. The foreign partner requests secondary information from USCIS in the event of a match in IDENT. USCIS relies on the foreign partner to provide accurate information. USCIS analysts verify the accuracy by comparing information provided by the foreign partner with information contained in the individual's A-File and from USCIS, DHS, and non-DHS systems. USCIS analysts compare information from various databases (i.e., CIS, PCQS, CPMS, EARM) and make annotations in ICTS showing any discrepancies. If a name is incorrect, for example, the name provided by the foreign partner will stay in ICTS (along with USCIS' response showing the name USCIS has for the individual) to show there were different names associated with this biometric, and thus, a potential fraud issue.

Section 3.0 Uses of the Information

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

3.1 Describe how and why the project uses the information.

USCIS uses ICTS to centralize the intake and processing of country-specific request templates from foreign partners. ICTS also tracks turnaround requirements based on the criticality of the required information requests.

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.

Not applicable.

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

No. Access to ICTS is limited to USCIS employees located at the NRC with a need-to-know. There are no other components with assigned roles and responsibilities within ICTS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information stored in ICTS may be used for purposes outside of the original purpose for which it was collected or that the information is disseminated inappropriately.

Mitigation: To mitigate the privacy risk of unauthorized use, all users are specifically granted access to the system. Only USCIS users who have a need to know the information in the system can gain access to ICTS, and their access to information contained within the system is restricted to what is necessary to perform specific job-related functions.

Additionally, all users' actions are recorded in the system. Users have all been informed that inappropriate use of the system or information contained therein could lead to adverse personnel action to include job loss. All users also receive training on the proper handling of information in accordance with applicable laws, regulations, and policy, including but not limited to the Privacy Act.

Section 4.0 Notice

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

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

USCIS provides general notice to individuals through the associated SORNs and this PIA. USCIS presents all individuals seeking immigration benefits with a Privacy Notice. The Privacy Notice located on the instructions for each form notifies individuals of USCIS authority to collect information, the purposes for the collection, routine uses of the collected information, and consequences of declining to provide the information to USCIS. Specifically, the Privacy Notice informs individuals that information may be shared with foreign partners in accordance with approved routine uses as described in the associated published system of records notices. Further, the information may also be made available, as appropriate for law enforcement purposes or in the interest of national security.

In addition, USCIS benefit applications and petitions require that applicants submit the necessary information, including biographic information, and when required, the submission of fingerprints and photographs. The instructions for certain immigration benefit forms notify the individual that biometric collection is required for the purpose of conducting background checks and that the information may be shared with foreign governments. Further, the instructions also advise the individual that the information is critical in making an informed adjudication decision

in granting or denying a USCIS benefit and that the failure to submit such information may prohibit USCIS from processing and properly adjudicating the form and thus preclude the benefit requestor from receiving the benefit.

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

Individuals who apply for USCIS benefits are presented with a Privacy Notice, and sign a release authorization on the benefit request. The Privacy Notice details the authority to collect the information requested. The forms also contain a provision by which a benefit requestor authorizes USCIS to release any information received from the benefit requestor as needed to determine eligibility for benefits. An individual may decline to provide his or her biometrics but is cautioned that failure to do so may make result in USCIS' inability to determine eligibility for the requested benefit. The Privacy Notice on benefit forms includes exchanging information with foreign partners.

4.3 Privacy Impact Analysis: Related to Notice

There is no privacy risk related to notice. All USCIS applicants and petitioners are provided notice prior to submitting any information to USCIS that information may be shared with foreign partners. The Privacy Notice for each form notes that USCIS may share information with foreign partners. USCIS also provides notice through the associated SORNs and publication of this PIA.

Section 5.0 Data Retention by the project

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

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

USCIS is working with NARA to develop a records retention schedule to cover the ICTS records. USCIS proposes to delete and destroy the information 6 years from the last completed action. Until there is a finalized retention schedule in place, USCIS cannot delete any records in ICTS.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Without an approved retention schedule, there is a risk that information may be retained longer than necessary and may increase the potential of an unauthorized disclosure.

Mitigation: USCIS is working to mitigate this risk. USCIS is developing a retention schedule for ICTS. The proposed NARA schedule is consistent with the concept of retaining data only for as long as necessary to support USCIS mission. Until USCIS completes a NARA-approved retention schedule, USCIS plans to maintain all records indefinitely in accordance with the Federal Records Act, which prohibits agencies from destroying records without a NARA-approved schedule.

Section 6.0 Information Sharing

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

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

Yes. DHS is a party to numerous international data sharing efforts in support the DHS mission.[28] The purpose of the Visa and Immigration Information Agreements is to support immigration processes, including asylum, visa, and refugee determinations, as well as admissibility, among the FCC partners. These agreements assist in the administration and enforcement of their immigration laws by furthering the prevention, investigation, or punishment of acts that would constitute a crime rendering a national of a third country inadmissible or removable under the immigration laws of the party providing the information.[29] Through the agreements, DHS shares biometric and associated biographic information with foreign partners through OBIM IDENT. At this time, USCIS is only receiving and responding to secondary queries from New Zealand, Canada, and Australia.

NPPD OBIM, through IDENT, supports the initial query and response process for international biometric sharing. The foreign partner initiates a fingerprint query in IDENT, then IDENT returns an automated response of "match" or "no match." If there is a match, limited biographic information contained in IDENT is provided.[30] If the foreign partner needs additional information to assist in the adjudication of the benefit, the foreign partner may request DHS for additional information. IDENT then returns limited biographic data associated with the matched identity. The foreign partner may need additional data on the matched individuals and may send an additional query. If USCIS is the original source of the match information contained in IDENT,

[28] DHS has signed MOUs in place with each partner country. Appendix A to this PIA outlines our current (although not all implemented) agreements with foreign partners.
[29] *See generally*, Visa and Immigration Information Sharing Agreements, art. 2.
[30] The specific data elements are outlined in the IDENT PIA.

the request is transmitted to CPMS. CPMS then sends the foreign partner query to ICTS. USCIS uses ICTS to receive and respond to foreign partner queries.

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

Sharing information with foreign partners is compatible with the purpose of the applicable system of records notice (noted in Section 2.1) because disclosure to foreign partners assists USCIS in adjudicating applications for immigration benefits. That purpose is the reason that USCIS needs this information.

Specifically, Routine uses G, P, Q, and II of the A-File SORN, Routine use G of the Background Check Service SORN, Routine use F of the Biometric Storage System SORN, Routine use G of the Benefit Information SORN, Routine Use J of Asylum Information and Pre-Screening, and Routine Use J of the Refugee Case Processing and Security Screening Information SORN permit USCIS to share information with foreign partners for the administration and enforcement of immigration, civil, or criminal laws.

6.3 Does the project place limitations on re-dissemination?

DHS enters into Memoranda of Understanding/Agreement (MOU/A) and Statement of Mutual Understanding (SMU), with foreign partners prior to the exchange sharing of information. The information sharing and implementing agreements between DHS and foreign partners fully outline responsibilities of the parties, security standards, and limits of use of the information, including re-dissemination, prior to information sharing. Access to records is governed by need-to-know criteria that demand the receiving entity demonstrate the mission-related need for the data before access is granted. Onward sharing is not permitted without prior approval by DHS.

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

The ICTS system maintains the records of disclosure outside of the Department as all requests for information. ICTS also tracks what information is disclosed and to whom the information was released. Information about the disclosure is also interfiled into the corresponding A-File.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: The primary privacy risk associated with external information sharing is the potential disclosure of data for purposes that are not in accord with the stated purpose and use of the original collection.

Mitigation: All international data sharing efforts are managed by International Integrated Project Team (IPT), which includes subject matter experts from impacted Programs and Directorates, the Office of Chief Counsel, and the Office of Privacy. The IPT monitors the development and implementation of new agreements and ensures protection of records through the development of system requirements and filtering tools. While DHS negotiates all international agreements, USCIS is included in the process and ensures that only permissible information is shared with foreign partners. As discussed above, ICTS maintains a record of disclosure of information in accordance with executed information sharing agreements. Additionally, the disclosure information is also interfiled into the A-File.

Privacy Risk: There is a risk that USCIS may disclose protected information inconsistent with the confidentiality requirements for T, U, and Violence Against Women Act (VAWA),[31] Asylum and Refugee information (i.e., 8 U.S.C. § 1367 and 8 U.S.C. § 208.6).

Mitigation: DHS employees are aware of the importance of safeguarding information protected by confidentiality provisions. USCIS is careful to share data only with external agencies that not only have a need-to-know but are also legally permitted to receive information covered under confidentiality provisions. There are different requirements depending on which special protected class is implicated. If USCIS shares information externally, it will only share the information in a way that is compatible with the statutory and regulatory confidentiality provisions and the relevant USCIS SORNs. Prior to disclosing any information USCIS employees are required to verify the status of an individual. USCIS enhanced the CIS and PCQS to tag records relating to a protected individual and that specific procedures regarding the disclosure and use apply to users accessing the information. CIS and PCQS include a banner to indicate that an individual is protected by confidentiality provisions. There are different banners for different special protected classes.

The law requires that USCIS protect information about principal applicants and their derivatives from disclosure in order to avoid endangering applicants and beneficiaries. These confidentiality protections generally continue indefinitely; they may terminate only when the application for relief is denied and all opportunities for appeal of the denial have been exhausted. Any record in CIS or PCQS that displays this banner must be handled in accordance with USCIS policy. ICTS allows USCIS analysts to indicate within the system whether the record subject is covered by confidentiality provisions. USCIS also created a standard operating procedure (SOP) that covers all filter rules for special protected data and how to appropriately respond to foreign partner requests about individuals who are covered by confidentiality laws.

[31] Victims of Trafficking and Violence Protection Act of 2000 (VTVPA), Pub. L. No. 106-386, 114 Stat. 1464 (2000).

Section 7.0 Redress

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

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

An individual seeking access to his or her information held by USCIS may gain access to his or her records by filing a Freedom of Information Act (FOIA) or Privacy Act request. Individuals not covered by the Privacy Act or Judicial Redress Act (JRA) still may obtain access to records consistent with 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 to access to his or her information should direct his or her request to the following address:

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

Further information for Privacy Act and FOIA requests for USCIS records can also be found at http://www.uscis.gov. Appendix A provides links to foreign partner redress processes.

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

U.S. citizens and lawful permanent residents, as well as other persons with records covered by the Judicial Redress Act (JRA), are afforded the ability to correct information by filing a Privacy Act Amendment request under the Privacy Act. U.S. citizens, lawful permanent residents, and persons covered by the JRA should submit requests to contest or amend information contained in ICTS as discussed in Section 7.1. Individuals may direct all requests to contest or amend information to the USCIS FOIA/PA Office. Individuals must state clearly and concisely in the redress request the information being contested, the reason for contesting it, the proposed amendment, and clearly mark the envelope "Privacy Act Amendment." This would only apply to amendment of USCIS-held information. Persons not covered by the Privacy Act are not able to amend their records through FOIA. Should a non-U.S. person find inaccurate information in his or her record received through FOIA, he or she may visit a local USCIS Field Office to identify and amend inaccurate records with evidence. Additionally, Appendix A provides links to foreign partner redress processes.

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

Individuals are notified about procedures for correcting their information by relevant USCIS application instructions, the USCIS website, this PIA, and relevant SORNs.

7.4 Privacy Impact Analysis: Related to Redress

There is no privacy risk with respect to redress. USCIS provides individuals multiple avenues during and after the completion of the benefit request process to correct information. There is a process to update records during the adjudication process. During the adjudication process, an officer may request a data edit. Individuals are given numerous opportunities during and after the completion of the benefit request process to correct information they have provided and to respond to information received from other sources. Information in ICTS is derived from other USCIS systems and from foreign partners. Appendix A provides links to foreign partner redress processes.

Section 8.0 Auditing and Accountability

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

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

USCIS ensures that practices stated in this PIA comply with internal USCIS policies, including the USCIS privacy policies, SOPs, information sharing agreements, orientation and training, rules of behavior, and auditing and accountability. All USCIS systems employ auditing measures and technical safeguards to prevent the misuse of data. Access and security controls have been established to mitigate privacy risks associated with authorized and unauthorized users, namely misuse, and inappropriate dissemination of data. DHS security specifications require auditing capabilities that log the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. In accordance with DHS security guidelines, USCIS systems use auditing capabilities that log user activity. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed.

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

USCIS employees and contractors are required to complete annual Privacy and Computer Security Awareness Training to ensure their understanding of proper handling and securing of PII. The Privacy Awareness training addresses appropriate privacy concerns, including Privacy Act obligations (e.g., SORNs, Privacy Act Statements). The Computer Security Awareness training examines appropriate technical, physical, personnel, and administrative controls to safeguard information.

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

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

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 developed an International IPT to manage all international data sharing efforts. The IPT monitors the development and implementation of new agreements and ensures protection of records through the development of system requirements and filtering tools. While DHS negotiates all international agreements, USCIS is included in the process and ensures that only permissible information is shared with foreign partners. Any new use of information or new access requests for the system must be approved by the proper authorities of this process such as the

USCIS Privacy Officer, Chief of Information Security Officer, Office of Chief Counsel, and the respective Program Office.

Responsible Officials

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

Approval Signature

Original, signed copy on file with the DHS Privacy Office

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

Appendix A

Organizations:

The Five Country Conference (FCC) is a forum for cooperation on migration and border security between the countries of Australia, Canada, New Zealand, the United Kingdom, and the United States (collectively called the FCC partners). At this juncture, USCIS is only automating the secondary request process for New Zealand, Canada, and Australia.

Purpose and Use:

The purpose of this information sharing is to support immigration processes, including asylum, visa, and refugee determinations, as well as admissibility, with New Zealand, Canada, and Australia. Foreign Partners perform search only in IDENT. If there is a no match to a record in IDENT, the system returns a "no-match" response to the foreign partner. However, if there is a match to data in IDENT, then the system sends the approved data elements and creates an encounter to an existing matched record. IDENT only adds encounters to an existing identity. FCC partners exchange their biometric data to search against the existing biometric holdings of other FCC partners to determine whether information pertinent to immigration and border management exists.

Individuals Impacted:

Individuals impacted include those encountered in the following immigration situations in an FCC partner country:

- When there is an indication of derogatory activity (e.g., child smuggling) or other associations of concern such that the individual could be found inadmissible to one or more of the FCC partner countries.
- When the identity of the individual is unknown (e.g., an individual who has destroyed his or her identifying documents or withheld information about his or her identity to prevent removal).
- When there is reason to believe that another FCC partner has encountered the individual.
- When there is an asylum claim that involves identifying individual(s) encountered inside the FCC partner country, or locating individuals whose whereabouts are unknown or who may have violated immigration or criminal laws.
- When an individual requires re-documentation for removal or another immigration-related process.

Data Elements:

In the event of an information match, two FCC partners (the requesting and providing countries) may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether further action is required using other existing protocols (law enforcement or otherwise) between the countries. USCIS may share information and supporting documentation about the record subject being requested by the foreign partner (e.g., current immigration status, application/petition history and decisions, prior immigration violations, and biographic information.

Partner Notice:

The following FCC partner countries have provided notice by posting PIAs on this data exchange:

- *Canada*: http://www.cic.gc.ca/english/department/atip/pia/fcc.asp.
- *Australia*: Australia conducts PIAs, but does not publicly post those documents.
- *New Zealand:* https://www.immigration.govt.nz/about-us/policy-and-law/identity-information-management/how-biometric-information-is-used.

Correction and Redress:

If an individual believes that the information held on him/her is incorrect, he or she may submit an inquiry to the following points of contact in each country:

- *Australia*: DIAC, Minister for Immigration and Citizenship, Local Member of Parliament, Commonwealth Ombudsman, or the Australian Privacy Commissioner.
- *Canada*: For access to personal information held by Citizenship and Immigration Canada, please refer to its website at: http://www.cic.gc.ca/english/department/atip/requests-personal.asp.
- *New Zealand**:*** Persons may also visit the Immigration New Zealand website for access, please refer to its website at: https://www.immigration.govt.nz/contact/request-information.

Onward Transfer:

Information received by any FCC partner is limited to determining the handling of an immigration case in that country only. FCC partners do not share information exchanged under this protocol with non-FCC partners without the permission of the FCC partner(s) that originally provided the information. For search requests resulting in matches against two or more countries, information may only be exchanged initially on a bilateral basis; however, the requesting country may inform each providing country about the existence of another matching record and the identity of the other FCC partner(s) with a matched record.

Training:

Privacy training for FCC partner participants complies with the appropriate training requirements defined by each FCC partner. All FCC Partner countries require that their employees complete Privacy and Security training.

Information Sharing Agreements:

Five Country Conference Agreements and Related Documentation include:

1. High Value Data Sharing Protocol Memorandum of Understanding between The Australian Department of Immigration and Citizenship (DIAC) and the United States Homeland Security and the United States Department of Homeland Security (DHS) and the United States Department of State (DoS).

2. Letter of Agreement to amend the High Value Data Sharing Protocol Memorandum of Understanding between The Australian Department of Immigration and Citizenship (DIAC) and the United States Homeland Security and the United States Department of Homeland Security (DHS) and the United States Department of State (DoS).

3. Agreement Between the United States of America and The Government of Australia For the Sharing of Visa and Immigration Information - Signed at Canberra August 27, 2014.

4. Implementing arrangement between Department of Immigration and Border Protection of Australia and DHS– Signed at London, September 9, 2015.

5. Disclosure of Asylum-Related Information to the Foreign Government Participants on the Five Country Conference," Secretary Napolitano, March 5, 2010.

6. Implementing Arrangement between the Department of State and the Department of Homeland Security of the United States of America, on the one side, And the Department of Citizenship and Immigration of Canada and the Canada Border Services Agency, on the other side, concerning Biometric Visa and Immigration Information Sharing (May 2015).

7. Annex to the 2003 Statement of Mutual Understanding on Information Sharing regarding the Sharing of Information Under the Five Country Conference High Value Data Sharing Protocol between the Department of Citizenship and Immigration Canada (CIC).

8. Disclosure of Asylum-Related Information to the Foreign Government Participants on the Five Country Conference, 2016.

9. The Agreement between the Government of Canada and the Government of the United States of America for the Sharing of Visa and Immigration Information (December 13, 2012).

10. Agreement between the Government of the United States of America and the Government of New Zealand for the Sharing of Visa and Immigration Information (Visa and Information Agreement) (May 4, 2017).

11. Implementing Arrangement between the Department of State and the Department of Homeland Security of the United States of America, on the one side, and the New Zealand Ministry of Business, Innovation and Employment, on the other side, concerning the sharing of visa and immigration information including on a systematic basis (Implementing Arrangement) (November 7, 2017).

Applicable Routine Uses:

The following Routine uses permit USCIS to share information with foreign partners for the administration and enforcement of immigration, civil or criminal laws:

DHS/USCIS/ICE/CBP-001 A-File SORN:[32]

G. To an appropriate federal, state, tribal, territorial, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations.

P. To appropriate federal, state, local, tribal, territorial, or foreign governments, as well as to other individuals and organizations during the course of an investigation by DHS or the processing of a matter under DHS's jurisdiction, or during a proceeding within the purview of the immigration and nationality laws, when DHS deems that such disclosure is necessary to carry out its functions and statutory mandates.

Q. To an appropriate federal, state, tribal, territorial, local, or foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence, whether civil or criminal, or charged with investigating, prosecuting, enforcing, or implementing civil or criminal laws, related rules, regulations, or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence and the disclosure is appropriate to the proper performance of the official duties of the person receiving the information.

II. To a federal, state, local, territorial, tribal, international, or foreign criminal, civil, or regulatory law enforcement authority when the information is necessary for collaboration, coordination, and de-confliction of investigative matters, prosecutions, and/or other law

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

enforcement actions to avoid duplicative or disruptive efforts and to ensure the safety of law enforcement officers who may be working on related law enforcement matters.

DHS/USCIS-002 Background Check Service SORN:[33]

G. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where USCIS believes the information would assist enforcement of civil or criminal laws.

DHS/USCIS-003 Biometric Storage System SORN:[34]

F. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where DHS determines that the information would assist in the enforcement of civil or criminal laws.

DHS/USCIS-007 Benefit Information System SORN:[35]

J. To appropriate federal, state, tribal, and local government law enforcement and regulatory agencies, foreign governments, and international organizations, as well as to other individuals and organizations during the course of an investigation by DHS or the processing of a matter under DHS jurisdiction, or during a proceeding within the purview of the immigration and nationality laws, when DHS deems that such disclosure is necessary to carry out its functions and statutory mandates to elicit information required by DHS to carry out its functions and statutory mandates.

DHS/USCIS-010 Asylum Information and Pre-Screening SORN:[36]

I. To other federal, state, tribal, and local government agencies, foreign governments, intergovernmental organizations and other individuals and organizations as necessary and proper during the course of an investigation, processing of a matter, or during a proceeding within the purview of U.S. or foreign immigration and nationality laws, to elicit or provide information to enable DHS to carry out its lawful functions and mandates, or to enable the lawful functions and mandates of other federal, state, tribal, and local government agencies, foreign governments, or intergovernmental organizations as limited by the terms and conditions of 8 CFR 208.6 and any waivers issued by the Secretary.

J. To a federal, state, tribal, or local government agency or foreign government seeking to

[33] DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007).
[34] DHS/USCIS-003 Biometric Storage System, 72 FR 17172 (April 3, 2007).
[35] DHS/USCIS-007 Benefit Information System, 81 FR 72069 (Oct. 19, 2016).
[36] DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (Nov. 30, 2015).

verify or ascertain the citizenship or immigration status of any individual within the jurisdiction of the agency for any purpose authorized by law as limited by the terms and conditions of 8 CFR 208.6 and any waivers issued by the Secretary pursuant to 8 CFR 208.6.

DHS/USCIS-017 Refugee Case Processing and Security Screening Information SORN:[37]

J. To requesting foreign governments under appropriate information sharing agreements and there is a legitimate need to share information for law enforcement or national security purposes under 8 CFR 208.6.

[37] DHS/USCIS-017 Refugee Case Processing and Security Screening Information System of Records, 81 FR 72075 (Oct. 19, 2016).