Privacy Impact Assessment
for the

Refugee Case Processing and Security Vetting

DHS/USCIS/PIA-068

July 21, 2017

Contact Point
Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
(202) 272-8000

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

Abstract

U.S. Citizenship and Immigration Services (USCIS) and the Department of State (DOS) work cooperatively to administer the overseas component of the U.S. Refugee Admissions Program (USRAP). The mission of the USRAP is to resettle eligible refugees in the United States. Although DOS has overall management responsibility for the USRAP, USCIS Refugee, Asylum and International Operations Directorate (RAIO) Refugee Affairs Division (RAD), and in some cases International Operations (IO) Division, is responsible for interviewing refugee applicants, receiving and reviewing results of all background checks, and adjudicating applications for refugee status. USCIS is conducting this Privacy Impact Assessment (PIA) because the USRAP collects, uses, and maintains personally identifiable information (PII) in support of refugee resettlement and employment eligibility. This PIA comprehensively covers current USRAP processes and procedures. USCIS will update and republish this PIA immediately should the USRAP vetting process change.

Overview

U.S. Citizenship and Immigration Services (USCIS), a component of the Department of Homeland Security (DHS), and the Department of State (DOS) collaborate to manage and operationalize the overseas component of the U.S. Refugee Admissions Program (USRAP). The USRAP is an interagency effort involving a number of governmental and non-governmental partners both overseas and in the United States. The mission of the USRAP is to resettle eligible refugees in the United States.[1] DOS has overall management responsibility for the USRAP and leads in proposing admissions ceilings and defining processing priorities under which individuals may obtain access to the USRAP. The USCIS Refugee, Asylum, and International Operations Directorate (RAIO) Refugee Affairs Division (RAD), and in some cases International Operations (IO) Division, is responsible for interviewing refugee applicants, receiving, and reviewing results of all background checks, and adjudicating applications for refugee resettlement.

[1] On March 6, 2017, President Trump signed Executive Order 13780 (EO), "Protecting the Nation from Foreign Terrorist Entry into the United States." In addition to temporarily halting refugee admissions, the EO directs the Secretary of Homeland Security to review USRAP application and adjudication processes and implement additional procedures deemed necessary to ensure the security of the United States. The EO is currently under litigation. USCIS has not altered any procedure within the refugee application process due to the EO. USCIS will publish an updated PIA should any processes outlined in this PIA changes with respect to refugee vetting.

Management of Refugee Cases and Information

Case Information Systems

Five separate Information Technology (IT) systems maintain the information necessary to process applications for refugee resettlement. These systems include the DOS Worldwide Refugee Admissions Processing System (WRAPS) and USCIS systems including the Enterprise Collaboration Network (ECN), the Refugee Case Manager (RCM), the Case and Activity Management for International Operations (CAMINO), and R-TRACK. WRAPS maintains information related to all individuals referred to the USRAP for resettlement. USCIS has read-only access to WRAPS. In addition to these systems, DHS and DOS share biographic and biometric information with other law enforcement and intelligence agencies that conduct security screening checks for refugee applicants. The purpose of this PIA is to describe the USRAP process and the information collected, used, maintained, and disseminated on individuals applying for refugee status.

The following systems and processes maintain personally identifiable information in support of refugee resettlement:

1. **DOS Worldwide Refugee Admissions Processing System (WRAPS)**

The Resettlement Support Centers (RSC)[2] collect and initially enter information from Form I-590, *Registration for Classification as Refugee*, into WRAPS.[3] Form I-590 is the application form by which a person seeks refugee classification and resettlement in the United States. WRAPS is the case management system for the refugee program. The RSCs scan and upload all refugee Form I-590 applications and supporting documents into WRAPS, in which they can be tracked.[4]

In addition to being used for case management, WRAPS also allows officers to electronically review files to evaluate certain types of cases placed on hold and approve cases digitally, rather than solely through the physical file. Through the Digital Approval Process, USCIS and DOS officers can digitally approve cases that have cleared all security checks and are eligible for resettlement from any location with an internet connection and WRAPS access,

---

[2] The U.S. Department of State's Bureau of Population, Refugees, and Migration (PRM) funds and manages nine RSCs around the world, operated by international and nongovernmental organizations and one U.S. interests section. Under PRM's guidance, the RSCs prepare eligible refugee applications for U.S. resettlement consideration.
[3] http://2001-2009.state.gov/documents/organization/101146.pdf.
[4] WRAPS is the DOS case management database used for all refugee applicants processed for resettlement consideration to the U.S. Please see the WRAPS PIA and SORN for more information on this system and the information it collects, uses, and maintains. Available at http://www.state.gov/documents/organization/101146.pdf. RPC, operated by DOS contractors, is the central data repository for all overseas and domestic resettlement operations. The RPC manages the WRAPS database.

including at Headquarters in Washington, D.C. and while on circuit ride overseas.

2. Enterprise Collaboration Network[5] (ECN)

The Refugee Affairs Division (RAD) uses the USCIS ECN, a DHS SharePoint-as-a Service platform, to organize and share case information within RAD among several different programmatic areas and division branches. RAD and IO also use the ECN to track refugee adjudications. USCIS stores refugee case information, including case number, case size, case region, case stage, applicant name, and applicant nationality on the ECN.

3. Refugee Affairs Division Case Manager (RCM)

In addition to WRAPS and the ECN, the Refugee Affairs Division uses RAD Case Manager (RCM). The purpose of RCM is to track NO Decision (NOD) cases,[6] which are placed on hold for further Headquarters review. This system works by transferring data between the WRAPS network and the RCM. In RCM, RAD analysts can see the list of cases that need action taken, and answer questions such as how long a case has been waiting for review. A supervisor assigns the cases in the RCM to the reviewer. Once a reviewer is assigned, he or she can see that case in his or her work queue through the RCM interface. All data can be entered through the interface itself, and all changes are logged to provide a complete record of the actions taken on each case. After all reviews are complete, the adjudication decision and analysis must be transferred back to WRAPS, as well as other parties that need to know if a hold has been lifted. The data that is stored in the RCM includes case number, case size, case region, applicant name, and applicant nationality.

4. Case and Activity Management for International Operations (CAMINO)

USCIS uses CAMINO[7] to support case management functions of certain form types for IO and serves as a technical platform for routing certain types of background and security checks, including results of checks of intelligence community holdings, and receiving responses for RAD. CAMINO is a secure, web-based, case management application designed to facilitate the processing of immigration applications and petitions received or adjudicated by IO. Refugee application data and biographic check results for the principal applicant, derivatives, beneficiaries,[8] and other family members are processed in DOS WRAPS and USCIS CAMINO.

---

[5] *See* DHS/ALL/PIA-059 Employee Collaboration Tools, *available at* www.dhs.gov/privacy. USRAP management of information was designed in accordance with DHS/ALL/PIA-59.
[6] NOD cases are refugee cases in which the officer placed the case on hold for additional review before final adjudication. RAD is responsible for resolution of NOD cases.
[7] *See* DHS/USCIS/PIA-051 Case and Activity Management for International Operations (CAMINO), *available at* www.dhs.gov/privacy.
[8] A derivative beneficiary is an alien who cannot be directly petitioned for, but who can follow-to-join or accompany the principal beneficiary based on a spousal or parent-child relationship.

USCIS processes applications for the adjustment of status, refugee travel documents, and follow-to-join benefit petitions received via the Form I-730, *Refugee/Asylee Relative Petition*, in USCIS CAMINO and CLAIMS 3.[9]

5. R-TRACK

R-TRACK is a case tracking tool that allows team leaders and other reviewers to input, monitor, update, and communicate refugee case statuses and decisions. RAD Team leaders use R-TRACK to accurately track statistics, case decisions, and officer performance, while the Policy Branch uses it to access and compile statistics on Terrorist-Related Inadmissibility Grounds (TRIG). Other RAD Headquarters branches, such as Regional Operations and Security Vetting & Program Integrity (SPVI), use R-TRACK to access information on case outcomes and statistics. The R-TRACK is available on the ECN.

Resettlement Support Centers: Information Collection and Processing

Resettlement Support Centers (RSC), which are funded and managed by DOS, carry out administrative and processing functions, such as file preparation, data collection, and out-processing activities during the refugee admissions process. Nine RSCs around the world, operated by international and nongovernmental organizations and one U.S. interests section, provide support to USRAP based on different geographic regions. RSCs conduct the initial prescreening interview with refugee applicants and initiate biographic checks.

During an in-person prescreening interview, the RSC assists refugee applicants with completing Form I-590, *Registration for Classification as Refugee*. The Form I-590 is the primary document in all refugee case files and is an integral part of the applicant's case file. It is the application form by which a person seeks refugee classification and resettlement in the United States. It documents an applicant's legal testimony (under oath) as to identity, refugee claim, as well as other pertinent information, including marital status, number of children, military service, organizational memberships, and violations of law, if any. RSC schedules interviews for refugee applicants with USCIS officers, and the completed Form I-590 is submitted to USCIS for processing.

USCIS Interview: Information Collection and Adjudications

USCIS officers conduct in-person interviews with each refugee applicant to elicit information about the applicant's claim for refugee status and admissibility. As a result of the interview, refugee applicants may be found eligible for resettlement to the United States, not eligible for refugee resettlement, or have their case placed on hold for further review of their

[9] *See* DHS/USCIS/PIA-051 CAMINO; DHS/USCIS/PIA-016(a) Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems, *available at* www.dhs.gov/privacy.

eligibility. At the time of the USCIS interview, a hard copy of the I-590 is provided to the USCIS officer, along with supporting documentation, if any.

During the interview, the USCIS Officer:

- Confirms the basic biographical data of the applicant and reviews all information collected on the Form I-590;
- Verifies that the applicant was properly given access to the USRAP;
- Elicits verbal testimony regarding the refugee claim;
- Reviews supporting documentation, if available;[10]
- Determines whether the applicant has suffered past persecution or has a well-founded fear of future persecution on the basis of race, religion, nationality, membership in a particular social group, or political opinion in his or her home country;
- Determines whether the applicant is admissible to the United States, whether the applicant is subject to the persecutor bar, and whether he or she has been firmly resettled in another country; and
- Reviews that status of security screening checks and requests additional checks, if needed.

At the time of interview, or before, USCIS officers use the USCIS LiveScan mobile device to digitally collect ten press-prints and rolled fingerprints and a photo of every applicant who is over 13.5 years and under 80 years of age. LiveScan sends the collected information to the Customer Profile Management Service (CPMS)[11] through the Enterprise Service Bus (ESB).[12]

Security Screening Checks: Information Dissemination and Use[13]

All refugee applicants, derivatives, and certain family members are subject to background checks. As part of the background check, refugees undergo a series of biographic and biometric checks. USCIS may also conduct enhanced review and screening of certain cases. In partnership

[10] Supporting documentation could include Office of the United Nations High Commissioner for Refugees (UNHCR) registration, passports, registrations with host government, court documents, documents demonstrating that the applicant meets the requirements for a priority designation, and other identity documents. UNHCR, also known as the UN Refugee Agency, is a United Nations program mandated to protect and support refugees at the request of a government or the UN itself and assists in their voluntary repatriation, local integration, or resettlement to a third country.
[11] The LiveScan software is mobile device used to capture biometrics at refugee camps. *See* DHS/USCIS/PIA-060 Customer Profile Management Service (CPMS), *available at* www.dhs.gov/privacy.
[12] *See* DHS/USCIS/PIA-008 Enterprise Service Bus (ESB), *available at* www.dhs.gov/privacy.
[13] *See* USCIS Refugee Processing and Security Screening for more information, https://www.uscis.gov/refugeescreening.

and close coordination with federal law enforcement and the intelligence community, these checks have developed over the program's history and have been continually reviewed and enhanced as additional resources become available to interagency partners. Additionally, in some instances these checks may involve reviewing social media to identify information on applicants related to national security concerns or eligibility determinations.[14]

Biographic and biometric checks occur at multiple stages throughout the process, including before and after USCIS interview, immediately before a refugee's departure to the United States, and upon arrival in the United States.

Biographic Checks

The screening of refugee applicants involves numerous biographic checks that are initiated by the RSCs and reviewed and resolved by USCIS. These include:

- **Department of State (DOS) Consular Lookout and Support System (CLASS)**[15] name checks are initiated by DOS for all refugee applicants at the time of pre-screening by the RSC. Name checks are conducted on the applicant's primary names as well as any variations of name used by the applicant. Possible matches to applicants are reviewed by USCIS. Evidence of the confirmed matches is forwarded for inclusion in the A-File. If there is a new name or variation developed or identified at any time in the process, RSC requests another CLASS name check on the new name, and the case is placed on hold until that response is received.
- **DOS Security Advisory Opinion (SAO)**[16] is a DOS-initiated biographic check conducted by the Federal Bureau of Investigation (FBI) and intelligence community partners. SAO name checks are initiated at the time of pre-screening by the RSC for the groups and nationalities designated by the U.S. Government as requiring this higher level check. SAOs are processed and a response must be received prior to finalizing the adjudication decision. If there is a new name or variation developed at the interview, USCIS requests that another SAO be conducted on the new name and the case is placed on hold until that response is received.
- **Interagency Check (IAC)** involves sharing biographic data, including names, dates of birth, and other data points of all refugee applicants within designated age ranges that is captured at the time of pre-screening with intelligence community partners for checks against their holdings. This screening procedure was initiated in 2008 and has expanded

[14] All social media reviews will comply with DHS Management Directive 110-01, *Privacy Policy for the Operational Use of Social Media*, and accompanying Instruction 110-01-001.
[15] *See* Consular Lookout and Support System (CLASS) PIA, *available at* http://www.state.gov/m/a/ips/c24223.htm.
[16] *See* Visa Opinion Information Service (VOIS), *available at* http://foia.state.gov/_docs/PIA/185304.pdf http://foia.state.gov/_docs/PIA/185304.pdf. *See also* STATE-39, Visa Records, 77 FR 65245 (Oct. 25, 2012).

over time to include a broader range of applicants and records. These checks occur throughout the process.

- **National Counterterrorism Center (NCTC):** Pursuant to the National Security Act of 1974, as amended, NCTC "serves as the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support." ESB will forward the vetting information electronically to U.S. Customs and Border Protection's (CBP) Unified Passenger (UPAX) system.[17] UPAX acts strictly as a conduit, which will pass the information through to NCTC and does not store any information. NCTC reviews the information and sends back results, which once again will be passed through CBP's UPAX strictly as a conduit to CAMINO. USCIS uses this information to assist in identifying terrorism-related grounds of inadmissibility. The "clear" or "not clear" results of the NCTC check are uploaded into CAMINO.
- **Social Media Reviews** are conducted on select applicant populations by USCIS Fraud Detection and National Security Directorate (FDNS).[18] Social media reviews include Facebook, Twitter, Instagram, and YouTube, along with general internet searches (e.g., Google). Social media checks are designed to identify publicly available information in applicants' social media postings that may impact eligibility for their immigration filing. This could include information related to their claim for refugee status, information indicating potential fraud (such as identity fraud or document fraud), or information regarding criminal activity or national security concerns that would impact eligibility and admissibility. USCIS may only look at publicly available information and will respect users' privacy settings.

  USCIS FDNS uses social media identifiers to conduct screening and vetting checks of refugee applicants from publicly available information on social media. The social media reviews for refugee applications are initiated with overt research.[19] This may include allegations of potential fraud and verification of information to establish eligibility for an immigration benefit. In certain instances when there are national security or public safety concerns with a refugee application and overt research would compromise the integrity of an investigation, FDNS may use masked monitoring[20] to review the applicant's publicly

[17] *See* DHS/CBP/PIA-006 Automated Targeting System, *available at* www.dhs.gov/privacy.
[18] FDNS is responsible for conducting the social media reviews on behalf of RAD. *Please See* DHS/USCIS/PIA-013-01 Fraud Detection and National Security Directorate (FDNS) for more information about its social media practices, *available at* www.dhs.gov/privacy.
[19] Overt Research means collecting information from social media without logging in or otherwise interacting with individuals through social media. Overt research does not include creating identities or credentials on social media.
[20] Masked Monitoring means using identities or credentials on social media that do not identify a DHS/USCIS

available social media accounts. Under no circumstance will DHS/USCIS violate any social media privacy settings in the processing of refugee applications. USCIS will update this PIA as use of social media in the refugee vetting process evolves.

Biometric Checks

The screening of refugee applicants involves numerous biometric checks that are initiated once USCIS digitally collects fingerprints, which are automatically uploaded to CPMS. CPMS sends fingerprints, photographs, and limited biographic information to the following biometric-based background and verification checks:

- **DHS Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT)**[21] is a biometric record check related to travel and immigration history for non-U.S. citizens, as well as for immigration violations and law enforcement and national security concerns. Enrollment in IDENT also allows Customs and Border Protection (CBP) to confirm identity at the port of entry. With all refugee prints enrolled in IDENT, CBP has the capability to compare the prints of arriving refugees with the prints taken overseas in order to confirm that the person who was interviewed and approved is the same person who is attempting to enter the United States.
- **Federal Bureau of Investigation (FBI) Fingerprint Check**[22] uses the Next Generation Identification (NGI) system's recurring biometric record checks pertaining to criminal history and previous immigration data. All FBI fingerprint check requests and responses are routed to NGI via the ESB and the Automated Biometric Identification System (IDENT). There is no direct connection between the FBI's NGI and CPMS.
- **Department of Defense (DoD) Automated Biometric Identification System (ABIS)**[23] holdings collected by global U.S. forces during the course of military operations. DoD collects information to support its military mission, detainee affairs, and force protection efforts; as well as its antiterrorism, special operations, stability operations, homeland defense, counterintelligence, and intelligence efforts around the world. Additionally, DoD ABIS enrolls information collected from non-U.S. citizens denied access to military posts.

---

affiliation, or otherwise concealing a government affiliation, to conduct research or general, operational awareness. Masked monitoring includes logging in to social media, but does not include engaging or interacting with individuals on or through social media (which is defined as Undercover Engagement).

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

[22] The FBI replaced its Integrated Automated Fingerprint Identification System (IAFIS) with the Next Generation Identification (NGI). Please see the Privacy Impact Assessment (PIA), Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Biometric Interoperability for more information, *available at* https://www.fbi.gov/foia/privacy-impact-assessments/iafis-ngi-interoperability-1.

[23] Department of Defense Detainee Biometric Information System, 72 FR 14534 (Mar. 28, 2007). Also Defense Biometric Services, 74 FR 48237 (Sept. 22, 2009).

DHS CBP's National Targeting Center-Passenger (NTC-P) conducts biographic vetting of all ABIS biometric matches (both derogatory and non-derogatory) against various classified and unclassified United States Government databases. All DoD fingerprint check requests and responses currently flow through CPMS via ESB. There is no direct connection between DoD ABIS and CPMS.

The results of the above-mentioned biometric checks are maintained in CPMS. The USCIS Refugee Affairs Division receives reports of individual fingerprint matches and reviews the records to determine whether the data impacts the refugee eligibility determination.

During the process of adjudicating any USCIS benefit, if any national security concerns are ever raised, either based on security and background checks or personal interviews or testimony, USCIS refers cases to SVPI to conduct an additional level of review.[24]

USCIS receives and stores "clear" or "not clear" results of background identity and security checks in WRAPS. This information includes only the date of the background check, whether the check returned any derogatory results, whether those results were resolved, and expiration date of the results. The CLASS name check (CNC) results are saved in the case file for each individual. The DOS-generated CNC forms do not include any information about the security checks process, or any information used to resolve each security check. A form is printed for each individual and saved in each individual's case file. As the security checks process continues, additional CNC forms are printed and saved in the individual's case file. After SAO, IAC, and fingerprint checks are finalized, a final CNC form is presented. All CNC forms are saved in the case file to show the evolution of the security checks. Classified derogatory information correlating to the results is shared with USCIS in the form of disseminated message traffic sent by the screening agency (i.e., NCTC, FBI, and other intelligence community partners) to USCIS, where it is reviewed by officers with appropriate levels of security clearance.

Post-Decision Processing

USCIS uses the information from the application, security checks, interview, and supplemental evidence to determine whether the refugee is suitable for the refugee benefit. USCIS has the option to approve or deny a refugee case. USCIS may favorably adjudicate a refugee application after security check results are received and cleared. USCIS may deny a refugee application if security checks are not clear or there are other reasons for denial that are not security-related. The Form I-590 shows that an applicant was interviewed by USCIS and records the decision made by the USCIS Officer as to whether the applicant should or should not be classified

[24] *See* DHS/USCIS/PIA-013-01 Fraud Detection and National Security Directorate (FDNS), *available at* www.dhs.gov/privacy.

as a refugee for the purposes of admission to the United States pursuant to Section 207 of the Immigration and Nationality Act.

USCIS refers eligible applicants to RSCs for out-processing and issuance of a transportation letter. RSCs process approved cases for travel, including scheduling medical exams and arranging sponsorship by a domestic resettlement agency. Paper documents are sent to the International Organization for Migration (IOM), and the Refugee Travel Packet is generated.[25] The Refugee Travel Packet contains the completed refugee application, completed employment eligibility application, transportation letter, Report of Medical Examination and Vaccination Record, travel document, and photographs for review by a DHS immigration official when the individual enters the United States.

After a refugee is authorized for travel to the United States, CBP receives a manifest of all individuals who have approved and have made reservations to travel to the United States by air. CBP receives this manifest before the scheduled travel. CBP performs initial vetting of the individuals before they arrive at a port of entry and the conducts both background checks and interviews of these individuals upon arrival at a U.S. Port of Entry. All refugee travel information collected on flight manifests is screened prior to boarding through the CBP National Targeting Center – Passenger (NTC-P)[26] and Transportation Security Administration (TSA) Secure Flight Program.[27] CBP also conducts TECS name checks[28] on approved refugee applicants seeking admission at ports-of-entry.[29] TSA, in coordination with CBP, conducts No Fly Selectee name and date of birth checks prior to the boarding of inbound aircraft. CBP determines if the applicant is admissible to the United States and if so, admits applicant to the United States as a refugee.

Upon arrival, the refugee applicant provides his or her Refugee Travel Packet to IOM). IOM hands the transportation letter from the Refugee Travel Packet and Form I-765, *Application for Employment Authorization* to CBP as evidence of lawful admission into the United States. CBP returns the transportation letter to the refugee applicant for onward travel, and returns the Form I-765 to IOM to interfile back to the refugee's travel packet. IOM ships all of the Refugee Travel Packets to the Nebraska Service Center (NSC) to process the Form I-765 and create the A-File.[30]

---

[25] International Organization for Migration (IOM), DOS contractors, serve primarily as the travel agent for USRAP. DOS Contractors make travel arrangements for refugees eligible for resettlement and assist them with travel and processing at the port of entry in the United States.
[26] *See* DHS/CBP/PIA-006(d) Automated Targeting System, *available at* www.dhs.gov/privacy.
[27] *See* DHS/TSA/PIA-018(h) Secure Flight Program and its respective updates, *available at* www.dhs.gov/privacy.
[28] *See* DHS/CBP/PIA-009(a) TECS System: CBP Primary and Secondary Processing (TECS), *available at* www.dhs.gov/privacy.
[29] Entry of refugees to the United States is limited to only six US International Air Ports of Entry: Chicago, Houston, Los Angeles, Miami, Newark, and New York.
[30] An A-File is a series of records maintained on an individual that document his or her history of interaction with USCIS, CBP, and Immigration and Customs Enforcement (ICE) as prescribed by the Immigration and Nationality Act (INA) and other regulations regarding immigration benefits. *See* DHS/USCIS/ICE/CBP-001 Alien File, Index,

Both the physical and electronic A-Files[31] are shipped to the National Records Center (NRC). The NRC securely stores A-Files for future retrieval.

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?

Section 207 of the Immigration and Nationality Act (INA), as amended,[32] provides the legal authority for refugee admissions to the United States.

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

The following SORNs cover the collection, maintenance, and use of the information for refugee resettlement:

- DHS/USCIS-017 Refugee Case Processing and Security Screening Information SORN covers the collection, use, maintenance, and dissemination of refugee data, to include application intake, biometric checks, interviews, and adjudication.[33]
- STATE-59 Refugee Case Records SORN covers the collection of information from individuals who have applied for admission to the United States as refugees that is stored in WRAPS. Routine Use 1 of STATE-59 Refugee Case Records permits DOS to share information with USCIS to determine the eligibility and admissibility of individuals applying for admission to the United States as refugees or any other immigration benefit under U.S. law. [34]
- DHS/USCIS-002 Background Check Service SORN covers background checks and their results;[35]

---

and National File Tracking System of Records, 78 FR 69864 (Nov. 21, 2013), *available at* www.dhs.gov/privacy.
[31] USCIS digitizes paper-based case files (A-Files) and stores them in the Enterprise Document Management System (EDMS). *See* DHS/USCIS/PIA-003(a) Integrated Digitization Document Management Program, *available at* www.dhs.gov/privacy.
[32] 8 U.S.C. § 1157.
[33] *See* DHS/USCIS-017 Refugee Case Processing and Security Screening Information, 81 FR 72075 (Oct. 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.
[34] *See* STATE-59 Refugee Case Records SORN, *available at* http://www.state.gov/documents/organization/102801.pdf.
[35] *See* DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007).

- DHS/USCIS-003 Biometric Storage Systems SORN covers background checks, background check results, and card production;[36]
- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking SORN covers the materials from the refugee case file, which are consolidated into the A-File after the individual is admitted to the U.S. at a Port of Entry or a final decision to deny refugee status has been made.[37] A-Files are created for individuals who are interviewed by a USCIS officer overseas.

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

Yes. The processing of refugee applications include the use of WRAPS, CAMINO, and ECN. WRAPS is the case management system for the refugee program and is located and operated by the Department of State's Refugee Processing Center. Because USCIS does not have its own system for the refugee program, all refugee matters are handled in WRAPS.

The USCIS ECN is hosted on the DHS SharePoint-as-a-Service framework. Both RCM and R-TRACK are systems developed within ECN. DHS completed the completed the security assessment and authorization documentation. SharePoint-as-a-Service was issued a three year Authority to Operations, which expires on May 28, 2018.

CAMINO is covered as a minor system 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 CAMINO, to be reviewed on a monthly basis and maintain its security posture to maintain its ATO.

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

Yes. DOS adheres to the WRAPS retention schedule [A-25-003]. WRAPS retains records online for five (5) years after the refugee's arrival in the United States or case inactivity, and then transfers records to offline storage. DOS retains records offline for ten (10) years. Records are deleted when fifteen (15) years old.

NARA approved the CAMINO retention schedule [N1-566-12-06] on April 17, 2013. CAMINO retains records 25 years from the date of the last completed action. Case files are stored in the A-File [N1-566-08-11]. A-File records are permanent, whether hard copy or electronic. DHS

[36] *See* DHS/USCIS-003 Biometric Storage System, 72 FR 17172 (Apr. 6, 2007).
[37] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (November 21, 2013).

transfers A-Files to the custody of NARA 100 years after the individual's date of birth.

USCIS is working with the USCIS Records Officer on finalizing a retention schedule for RCM.

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.

The following forms used in support for refugee resettlement are subject to the Paperwork Reduction Act:

- Form I-590, *Registration for Classification as* Refugee (OMB No. 1115-0057).
- Form I-765, *Application for Employment Authorization* (OMB No. 1615-0040).

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.

Information about benefit requestor and derivatives may include:

- Full name;
- Alias(es);
- Physical and mailing addresses;
- Date of birth;
- Place of birth;
- Gender;
- Ethnicity or tribal group;
- Religion;
- Present Citizenship or Nationality;
- Alien Number (A-Number);
- Resettlement Support Center Case Number;

- Receipt Number;
- USCIS Online Account Number;
- Social Security number (SSN), if any;
- Relationship to benefit requestor (*i.e.*, children under the age of 21 and spouse);
- Employment authorization eligibility and application history;
- Records regarding organization membership or affiliation;
- Supporting documentation as necessary (*e.g.*, birth, marriage, divorce certificates; licenses; academic diplomas; academic transcripts; appeals or motions to reopen or reconsider decisions; explanatory statements; and unsolicited information submitted voluntarily by the applicant or family members in support of a benefit request);
- Government-issued identification (*e.g.*, passport, driver license);
- Notices and communications (including: Receipt notices; Requests for Evidence; Notices of Intent to Deny; and Proofs of benefit);
- Phone and fax numbers;
- Email addresses;
- Social media handles, associated identifiable information, and results;
- Marital status;
- Place of marriage;
- Arrival/Departure information;
- Immigration history (*e.g.*, citizenship/naturalization certificate number, removals, explanations);
- Family relationships (*e.g.*, parent, spouse, sibling, child, other dependents);
- Relationship practices *(e.g.*, polygamy, custody, guardianship);
- Personal background information (*e.g.*, involvement with national security threats, criminal offenses, Communist party affiliation, activity and/or affiliation with groups or organizations abroad, torture, genocide, killing, injuring, forced sexual contact, limiting or denying others religious beliefs, service in military or other armed groups, work in penal or detention systems, weapons);
- Health information (*e.g.*, vaccinations, referrals, communicable diseases, physical or mental disorders, prostitution, drug or alcohol abuse);

- Employment authorization eligibility and application history;
- Professional accreditation information;
- Financial information (*e.g.*, income, expenses, scholarships, savings, assets, property, financial support, supporter information, life insurance, debts, encumbrances, tax records);
- Travel history;
- Explanation/description of foreign travel;
- Education history;
- Work history;
- Documents establishing identity and claimed relationship (*e.g.*, marriage record, civil or criminal history, medical records, education records, DNA results);
- Physical description (*e.g.*, height, weight, eye color, hair color, race, ethnicity, identifying marks like tattoos or birthmarks);
- Biometrics (*i.e.*, fingerprints and photographs) and other related information (*e.g.*, race, ethnicity, weight, height, eye color, hair color);
- Background check results;
- Reports of investigations or derogatory information obtained from DHS and other federal systems;
- Refugee interview notes and assessments;
- Information regarding the status of Department of Justice (DOJ), Executive Office of Immigration Review (EOIR) proceedings, if applicable; and
- Case processing information such as date applications were filed or received by USCIS; application/petition status, location of record, other control number when applicable, and fee receipt data.

Information about the benefit requestor's parents and relatives in the United States and other individuals listed as part of the family tree and including points of contact in the United States and other individuals with whom the applicant associates:

- Name;
- Date of Birth;
- Relationship to the benefit requestor;

- Country of Birth;
- Address; and
- Background check results.

Information about Registrants, Preparers, and Interpreters may include:

- Full name;
- Organization;
- Business State ID number;
- Employer Tax Identification Number;
- Physical and mailing addresses;
- Email address;
- Phone and fax numbers;
- Relationship to applicant; and
- Signature.

Information about Accredited Representatives and Attorneys includes:

- Name;
- Law Firm/Recognized Organization;
- Physical and mailing addresses;
- Phone and fax numbers;
- Email address;
- Attorney Bar Card Number or equivalent;
- Bar membership;
- Accreditation date;
- Board of Immigration Appeals Representative Accreditation;
- Expiration date;
- Law Practice Restriction Explanation; and
- Signature.

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

Most of the information is derived from the data provided by the refugee applicant on the completed Form I-590 in support of his or her application. USCIS also collects information from the in-person interview, internal DHS systems, and external systems during the security vetting process.

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

Yes. In some instances publicly available social media information can be accessed by authorized USCIS personnel trained to conduct social media review and used by adjudicators to evaluate a subject's biographic history, claims of persecution, and association with any known terrorists or terrorist organizations. This information is handled in a manner consistent with existing USCIS policies and rules of behavior regarding the use of social media information in adjudicative decision making.[38]

2.4 Discuss how accuracy of the data is ensured.

Accuracy of the data recorded on the I-590 and any other forms in support of refugee resettlement and employment eligibility is verified in-person with the applicant by RSC staff. Data is reviewed again for accuracy during in-person interviews conducted by USCIS officers with the applicant. When required, interpreters are used. Interpreters hired by the RSC are under oath. Interpreters sign the I-590, and the applicant attests on the form, if an interpreter is used, that he or she has understood the interpretation.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of over-collection of information during the interview process.

Mitigation: The USCIS Office of Privacy reviews each immigration form during the form development process and/or promulgation process to ensure that only the minimum amount of

[38] All FDNS personnel receive the USCIS Privacy Requirements for the Operational Use of Social Media training and sign Rules of Behavior before initial use is granted and annually thereafter. FDNS personnel also receive annual privacy awareness and program-specific training that reinforces the privacy principles. FDNS personnel may use masked accounts with the approval of their supervisor, when necessary to view publicly available information, and will receive hands-on training on the proper use of any tools or tradecraft used to access social media sites. *See* DHS Management Directive 110-01, *Privacy Policy for the Operational Use of Social Media*, and accompanying Instruction 110-01-001.

information is collected to determine benefit eligibility. Furthermore, all data elements collected are negotiated with and approved by OMB during PRA collection review. Form I-590 requires the information collected and stored to establish the identity of the refugee applicant or beneficiary and to process the benefit request to determine benefit eligibility. USCIS officers interviewing refugee applicants collect information that is required for adjudication of the refugee application according to U.S. law.

Privacy Risk: There is a risk of obtaining inaccurate data due to manual data entry.

Mitigation: This risk is mitigated. RSC staff manually enter the refugee applicant data directly into fields in WRAPS. The RSC generates the I-590 by using a functionality in WRAPS that pulls information from those fields in WRAPS to autopopulate to corresponding fields in the I-590. RSC staff review accuracy of the data on the I-590. Data is reviewed again for accuracy during in-person interviews conducted by USCIS officers with the applicant. If inaccurate information is identified during the interview, it is incumbent on the USCIS officer to correct the information in red ink on the I-590, review any corrections or annotations with the applicant, and obtain the applicant signature. After USCIS interview, RSC staff scan this updated version of the I-590 into WRAPS. When required, interpreters are used. Interpreters hired by the RSC work under oath. Interpreters sign the I-590, and the applicant attests on the form, if an interpreter is used, that he or she has understood the interpretation.

Privacy Risk: USCIS will rely on inaccurate information coming from social media to make a decision.

Mitigation: This risk is partially mitigated. Information is collected directly from applicants, and individuals generally have some degree of control over what is posted on their social media account. USCIS presumes some of this information is accurate. During the interview, the officer will review any social media assessments provided by FDNS, including those with possible inaccurate information, and address the underlying eligibility concern as annotated on the social media assessment with the applicant and elicit testimony as indicated. FDNS has also indicated that officers may provide the applicant with an opportunity to view the social media post (the post only, not the entire FOUO social media assessment) and provide additional testimony explaining any postings. Information collected from social media, by itself, will not be a basis to deny refugee resettlement and employment eligibility. USCIS has also developed procedures and training focused on understanding data quality limitations associated with social media.

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 the information that the RSC collects via the Form I-590, in prescreening, during in-person eligibility interviews, and biometric and biographic checks, in order to determine eligibility for refugee resettlement in the United States.

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

No.

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

No. Access to refugee records is limited to USCIS, DOS, and RSC employees with a valid need-to-know. The completed forms are handled by RSC staff and are stored on the Department of State's web database, WRAPS. USCIS, DOS, and the RSC have can see, but not edit, the forms in WRAPS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that collected information may be used for a purpose incompatible with the original purpose of collection.

Mitigation: Information related to refugee processing is kept confidential. The federal regulations at 8 CFR § 208.6 (a), govern confidentiality of asylum information, and by DHS policy also govern the general prohibition against disclosing refugee information to third parties. During the refugee interview, all applicants age 14 and older are asked to sign a consent to release information as part of the Form I-590, which allows sharing of information in limited circumstances. Signing this segment of the Form I-590 is voluntary. By signing this segment of the Form I-590, the applicant authorizes USCIS to release information contained in or pertaining to an application for refugee status necessary for the for the adjudication of the administration of U.S immigration laws and to the United Nations High Commissioner for Refugees (UNHCR), other United States Government agencies, and other resettlement countries. Interpreters that translate in refugee interviews sign a certification acknowledging that they are required to maintain confidentiality and to not disclose refugee information. No information is shared with the government of the country from which the applicant is seeking refuge, except under exigent

circumstances related to counterterrorism and national security.[39] Officers receive highly specialized training related to refugee processing and keep all information collected during refugee processing confidential. Additionally, standard operating procedures and policy guidance ensure that collected information is not used for a purpose incompatible with the original purpose of collection.

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 individuals general notice through this PIA and associated SORNs. Additionally, individuals who file Form I-590, *Registration for Classification as Refugee,* are presented with a Privacy Notice by DOS. The Privacy Act Notice details the authority to collect the requested information and outlines the intended uses. The form also contains a provision by which an applicant authorizes DOS to release any information received from the individual to USCIS as needed to determine refugee eligibility. Additional information about refugee processing is also available on the USCIS webpage.

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

Form I-590 requires the principal applicant to provide biographic information regarding his or her parents, current and or former spouses, fiancé (if any), and children. Principal applicants who file Form I-590 have an opportunity and the right to decline to provide information. However, the failure to submit such information precludes USCIS from processing the request for refugee status. By filing Form I-590, individuals have consented to the use of the information provided on the form by USCIS to determine their eligibility for refugee status.

4.3 Privacy Impact Analysis: Related to Notice

There is no privacy risk associated with notice because all information is provided voluntarily and USCIS provides notice to individuals through a Privacy Notice, this PIA, associated SORNs, and the USCIS website.

[39] See "Disclosure of Asylum or Refugee Information for Counterterrorism and Intelligence Purposes," Directive 262-02-01, § VI. A.2.b, issued November 15, 2016.

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.

DOS adheres to the WRAPS retention schedule [A-25-003]. WRAPS retains records online for five (5) years after the refugee's arrival in the United States or case inactivity, and then transfers records to offline storage. DOS retains records offline for ten (10) years. Records are deleted when fifteen (15) years old.

NARA approved the CAMINO retention schedule [N1-566-12-06] on April 17, 2013. CAMINO retains records 25 years from the date of the last completed action. Case files are stored in the A-File [N1-566-08-11]. A-File records are permanent, whether hard copy or electronic. DHS transfers A-Files to the custody of NARA 100 years after the individual's date of birth.

USCIS is working with the USCIS Records Officer on finalizing a retention schedule for RCM. Until USCIS and NARA finalize a retention schedule for RCM, USCIS maintains the records permanently.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information from internal refugee case information systems could be retained longer than needed.

Mitigation: This risk is partially mitigated. Officers receive specialized training on the use of internal refugee case information systems such RAD ECN page as well as other non-internal systems such as CAMINO. Records contained within CAMINO are maintained for 25 years. The information contained within ECN is used for internal communications within RAD and is maintained for as long as it is relevant. USCIS is working to mitigate the retention risk with respect to RCM by working with the USCIS Records Officer to finalize a retention schedule for RCM. Until USCIS completes a NARA-approved retention schedule for these records, 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. Refugee information and records may be shared with outside entities, either pursuant to regulation or through specific agreements.

Department of State (DOS)

DOS and USCIS share information as part of normal agency operations for processing refugee cases. Information sharing with DOS regarding refugee decisions includes notification of approval or denial of application. The decision to approve or deny an application is maintained in WRAPS and the RSC accesses this decision information to prepare the refugee cases for travel.

National Counter Terrorism Center (NCTC)

DHS has entered into an updated Memorandum of Agreement (MOA) with NCTC in order to facilitate NCTC's counterterrorism efforts and to identify terrorism information within WRAPS. Pursuant to 8 CFR § 208.6(a) as applied by policy to refugees, the Secretary has authorized regular sharing of refugee-related information for this purpose. This information sharing also aligns with DHS's mission to prevent and deter terrorist attacks and helps to ensure that immigration benefits are not granted to individuals who pose a threat to national security.

DOS provides the applicant's information via DOS WRAPS to USCIS through the Enterprise Service Bus (ESB) and onward for ingestion into CAMINO. USCIS also passes refugee information from DOS WRAPS to CBP UPAX, which serves as a technical pass through, providing the information to NCTC which may result in a match to derogatory holdings, when it exists. Any information that is returned by UPAX is sent to CAMINO, which is then used by USCIS personnel to compile and provide a final response to DOS WRAPS.

Department of Defense (DoD)

Pursuant to a MOA between DoD and DHS, biometric information is shared between USCIS and DoD to support the missions of both agencies. USCIS collects biometrics from refugee applicants and those biometrics are transmitted to DoD ABIS. DoD ABIS then conducts a search of all ABIS record categories on the received biometrics. All DoD fingerprint check requests and responses are maintained in CPMS.

Department of Justice (DOJ) Federal Bureau of Investigation (FBI)

USCIS sends certain refugee applicant information (*i.e.*, name, A-Number or SSN, date of birth, country of birth, race, gender, physical characteristics, address, reason for fingerprint, and fingerprint and facial photo images) to the FBI to conduct the fingerprint checks.

Intelligence Community

USCIS may send appropriate data to its partners in the intelligence community. This sharing may match to derogatory holdings, if it exists.

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

Department of State (DOS)

Sharing USCIS data with DOS is compatible with the purpose of the system because the DOS mission, like USCIS, includes ensuring refugee resettlement to the United States as dictated by the INA. Routine Use H of the Refugee Case Processing and Security Screening Information SORN[40] to share information with DOS when necessary to accomplish refugee case processing. Routine Use O of the A-File SORN[41] permits USCIS to share information with DOS for the purpose of processing of petitions or applications for benefits under the INA, and all other immigration and nationality laws including treaties and reciprocal agreements.

National Counter Terrorism Center (NCTC) and Intelligence Community

Sharing information with NCTC is compatible with the purpose of the system because USCIS is required to conduct background and security checks to identify threats to national security and public safety posed by those seeking refugee statuses. Routine Use I of the Refugee Case Processing and Security Screening Information SORN and EE of the A-File SORN permit USCIS to share information with NCTC or to any element of the U.S. intelligence community, or any other federal or state agency having a counterterrorism function, provided that the need to

[40] *See* DHS/USCIS-017 Refugee Case Processing and Security Screening Information, 81 FR 72075 (October 19, 2016).
[41] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (November 21, 2013).

examine the information or the request is made in connection with its authorized intelligence or counterterrorism function or functions and the information received will be used for the authorized purpose for which it is requested.

Department of Defense (DoD)

Sharing information with DoD is compatible with the purpose of the system because USCIS is required to conduct background and security checks to identify threats to national security and public safety posed by those seeking refugee statuses. Routine Use H of Background Check System, Routine Use I of the Refugee Case Processing and Security Screening Information SORN, and Routine Use EE of the A-File SORN permit USCIS to share information with DoD or to any element of the U.S. intelligence community, or any other federal or state agency having a counterterrorism function, provided that the need to examine the information or the request is made in connection with its authorized intelligence or counterterrorism function or functions and the information received will be used for the authorized purpose for which it is requested. USCIS conducts this vetting to determine if information exists that might render the individual ineligible for the benefit being sought.

Department of Justice (DOJ) Federal Bureau of Investigation (FBI)

Sharing information with the FBI is compatible with the purpose of the system because USCIS is required to conduct background and security checks to identify threats to national security and public safety posed by those seeking refugee statuses. Routine Use H of Background Check System, Routine Use I of the Refugee Case Processing and Security Screening Information SORN, and Routine Use EE of the A-File SORN permit USCIS to share information with NCTC or to any element of the U.S. intelligence community, or any other federal or state agency having a counterterrorism function, provided that the need to examine the information or the request is made in connection with its authorized intelligence or counterterrorism function or functions and the information received will be used for the authorized purpose for which it is appropriate to the proper performance of the official duties of the person making the disclosure requested. USCIS conducts this vetting to determine if information exists that might render the individual ineligible for the benefit being sought.

6.3 Does the project place limitations on re-dissemination?

DHS or USCIS enters into Memoranda of Understanding/Agreement (MOU/A) with external organizations prior to the systematic sharing of information. When sharing information with parties outside of DHS, the same specifications related to security and safeguarding of privacy-sensitive information that are in place for USCIS and DHS are applied to the outside entity. The agreements between DHS and external entities (*e.g.*, DOJ, DoD, DOS, and NCTC) fully outline responsibilities of the parties, security standards, and limits of use of the information, including re-dissemination, prior to information sharing. Access to records is governed by need-

to-know criteria that demand the receiving entity demonstrate the mission-related need for the data before access is granted. In the terms of a negotiated agreement or the language of an authorization providing information to an external agency, USCIS includes justification for collecting the data, and an acknowledgement that the receiving agency will not share the information without USCIS or DoS's permission, as applicable.

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

USCIS keeps an electronic record of all refugee records sent to non-DHS partners through CPMS and CAMINO audit and transactional logs.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk of misuse, unauthorized access to, or disclosure of information by DOS.

Mitigation: USCIS and DOS are partners in the processing of refugee cases. It is essential that information be shared between the two agencies for refugee resettlement. All personnel within DOS and USCIS are trained on the appropriate use and safeguarding of data. In addition, DOS and DHS have an MOU in place that as a general matter describes policies and procedures to prevent unauthorized dissemination of information. Any disclosure of information must be compatible with the purpose for which the information was originally collected and adhere to the confidentiality provisions of 8 CFR § 208.6 as applied by policy to refugee information. Only authorized USCIS users with a need to know may access the information.

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

Mitigation: USCIS is careful to share data with external agencies that have a need to know and put the information to a use that is compatible with the associated SORNs. The MOU/A also stipulates that USCIS is to be coordinated with prior to the dissemination of data to third parties. USCIS documents these safeguards in information sharing agreements with the external partners. All prospective information handlers must be authorized and trained to access the information. This mitigates the risk of unauthorized disclosure by requiring a trained employee with access to the information to review the information before sharing the information with an external agency.

Section 7.0 Redress

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

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

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

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

The information requested may be exempt from disclosure under the Privacy Act or FOIA because information may contain law enforcement sensitive information, the release of which could possibly compromise ongoing criminal investigations. Further information about Privacy Act and FOIA requests for USCIS records is available at http://www.uscis.gov.

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

Individuals who are United States citizens or lawful permanent residents should submit requests to contest or amend information as discussed in Section 7.1. The requestor should clearly and concisely state the information being contested, the reason for contesting or amending it, and the proposed amendment along with any evidence. The requestor should also clearly mark the envelope, "Privacy Act Amendment Request." The record must be identified in the same manner as described for making a request for access. Persons not covered by the Privacy Act are also able to amend their records. If a person finds inaccurate information in his or her record received through FOIA, he or she may visit a local USCIS Field Office to identify and amend inaccurate records with evidence. Individual refugee applicants located abroad may inform PRMs overseas partners of the need to correct inaccurate information. Refugee applicants inform these overseas partners of the error either by phone, in person or via email. PRM partners can then make the correction directly in WRAPS.

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

USCIS notifies individuals of the procedures for correcting their information in this PIA, 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 Act Statements, including notice of an individual's right to correct information, are also contained on the instructions to immigration forms published by USCIS.

7.4 Privacy Impact Analysis: Related to Redress

There is no risk associated with redress. USCIS provides individuals with access to their records that are not subject to exemptions when requested through a FOIA or Privacy Act request. Individuals who are United States citizens or lawful permanent residents may submit a Privacy Act requests to contest or amend information. Any person, regardless of immigration status can come to a USCIS Field Office or PRM overseas partner to identify or amend inaccurate records.

Section 8.0 Auditing and Accountability

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

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

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

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

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

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

USCIS employs 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.

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 the DHS Headquarters (including Office of General Counsel, Civil Rights and Civil Liberties, 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 Officials

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

Approval Signature

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

_____

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