Privacy Impact Assessment
for the

Citizenship & Immigration Data Repository (CIDR)

DHS/USCIS/PIA-031(a)

January 3, 2017

Contact Point
Tim Badger
Special Assistant, Program Management Office
Fraud Detection and National Security Directorate
U.S. Citizenship and Immigration Services
(202) 272-1047

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

Abstract

U.S. Citizenship and Immigration Services (USCIS) developed the Citizenship and Immigration Data Repository (CIDR) to enable authorized USCIS users to efficiently query between multiple USCIS benefits administration systems from a single entry point. CIDR allows for the vetting of USCIS application information for indications of possible immigration fraud and national security concerns, detecting possible fraud and misuse of immigration information or position by USCIS employees for personal gain or by coercion, and responding to requests for information (RFI) from the DHS Office of Intelligence and Analysis (I&A) or the federal intelligence community (IC) and law enforcement community (LE) members that are based on classified criteria. USCIS recently published an updated Privacy Impact Assessment (PIA) in January 2017 to evaluate the privacy risks and mitigations associated with the collection, use, and maintenance of personally identifiable information (PII) captured by CIDR. USCIS is now updating and reissuing the PIA with the following minor modifications: (1) to update USCIS' proposed retention period for background check related records and (2) to add language to reflect how long CIDR will retain audit trail information.

Overview

U.S. Citizenship and Immigration Services (USCIS) collects personally identifiable information (PII) directly from individuals, both citizens and noncitizens, through applications and petitions for the purposes of adjudicating and granting immigration benefits, requests, or services. USCIS maintains a number of electronic systems to facilitate these purposes, including: the Computer Linked Application Information Management System 3 (CLAIMS),[1] CLAIMS 4,[2] the Refugees, Asylum, and Parole System (RAPS) Asylum Pre-screening System (APSS),[3] Re-

[1] CLAIMS 3 is an electronic case management application that tracks and 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. For more information, *see* DHS/USCIS/PIA-016(a) Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems, *available at* www.dhs.gov/privacy.

[2] CLAIMS 4 is an electronic case management application tracking and processing system used as automated support for the variety of tasks associated with processing and adjudicating N-400, *Applications for Naturalization*. For more information, *see* DHS/USCIS/PIA-015 Computer Linked Application Information Management System 4 (CLAIMS 4) Update, *available at* www.dhs.gov/privacy.

[3] RAPS is used to verify the status of asylum applicants, asylees, and their dependents, to assist with the verification of an individual's immigration history in the course of a review of visa petitions and other benefit applications as well. APSS supports USCIS in the screening of individuals in the expedited removal process and of individuals subject to reinstatement of a final order of removal or an administrative removal order based on a conviction of an aggravated felony to determine whether they have credible fear or reasonable fear. For more information, *see* DHS/USCIS/PIA-027 Refugees, Asylum, and Parole System (RAPS) and the Asylum Pre-Screening System (APSS) Update, *available at* www.dhs.gov/privacy.

engineered Naturalization Application Casework System (RNACS)[4], Central Index System (CIS)[5], and the Fraud Detection and National Security Data System (FDNS-DS).[6]

USCIS developed CIDR, hosted on DHS classified networks, in order to make information from these USCIS systems available to authorized USCIS personnel for the following purposes: (1) vetting USCIS application information for indications of possible immigration fraud, public safety, and national security concerns; (2) detecting possible fraud and misuse of immigration information or position by USCIS employees, for personal gain or by coercion; (3) and responding to requests for information (RFI) from the DHS Office of Intelligence and Analysis (I&A) or law enforcement (LE) and the Intelligence Community (IC) that are based on classified criteria.

USCIS personnel carry out a number of steps to ensure that an individual is eligible as a matter of law and as a matter of discretion for a requested benefit or service. One of these steps is the performance of background, identity, and security checks to make certain that an individual is not attempting to obtain the requested benefit by fraudulent means or does not pose a public safety threat or a threat to national security.[7] Any related concerns identified during the adjudicative process are referred to the Fraud Detection and National Security Directorate (FDNS) for vetting and resolution.[8] This process identifies individuals who may be involved with benefit fraud, pose a risk to public safety or national security, or who otherwise may be ineligible for the immigration benefits sought.

Enhancing Existing Vetting Capabilities

CIDR enhances USCIS's existing vetting capabilities through several key functions. First, CIDR allows USCIS to more efficiently identify fraud, public safety, and national security concerns by allowing FDNS officers to review unclassified application data and related classified material, such as national security information identified in response to background checks, simultaneously. One background check that USCIS performs is a name-based check against the Federal Bureau of Investigation's (FBI) Central Records System (CRS) and Universal Index (UNI).[9] When a concern is identified that includes national security information, the FBI sends the

[4] USCIS decommissioned RNACS in 2013. However, the Enterprise Citizenship and Immigrations Services Centralized Operation Repository (eCISCOR) acts as a data repository for the decommissioned data. *See* DHS/USCIS/PIA-023(a) Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR), *available at* www.dhs.gov/privacy.
[5] CIS is a repository of electronic data that summarizes the history of an immigrant in the adjudication process. For more information, *see* DHS/USCIS/PIA-009 Central Index System (CIS), *available at* www.dhs.gov/privacy.
[6] *See* DHS/USCIS/PIA-013(a) Fraud Detection and National Security Data System (FDNS-DS), *available at* www.dhs.gov/privacy.
[7] During the adjudication process, USCIS conducts four different background checks; two biometric fingerprint based and two biographic name-based, which are discussed in detail in the Immigration Benefits Background Check Systems (IBBCS) PIA. *See* DHS/USCIS/PIA-033 IBBCS, *available at* www.dhs.gov/privacy.
[8] *See* DHS/USCIS/PIA-013-01 FDNS Directorate, *available at* www.dhs.gov/privacy.
[9] The FBI Name Check process is fully described in the USCIS Customer Profile Management System (CPMS) PIA. *See* DHS/USCIS/PIA-060 CPMS, *available at* www.dhs.gov/privacy.

classified results to USCIS via a classified email network, which USCIS then ingests into CIDR, making the data searchable and allowing FDNS officers to cross-reference that data with unclassified data found in other USCIS data sets.

Second, CIDR is a collaborative tool that enables multiple users to work on the same case. Thus, if an FDNS officer is working a fraud, public safety, or national security case in one location, a second officer may add information to the case elsewhere in the country. As most FDNS officers are located in Field Offices throughout the United States, this helps with case resolution.

Third, CIDR has a federated query capability that allows users to perform single, batch, and daily queries, returning results from the different immigration benefit datasets; CLAIMS 3, and in future releases, CLAIMS 4, RAPS, APSS, RNACS, and CIS. More importantly, a federated search capability links all of the data sets together, making it possible to search one system to determine what, if any, immigration benefit or service a person applied for or received. CIDR users who are FDNS officers can also search the metatag data fields of the FBI name check responses and RFIs.

Fourth, CIDR uses filters based on existing immigration fraud lead reports to narrow search parameters to specific data fields and to identify basic fraud patterns. These patterns are identified in accordance with FDNS and USCIS policy. Based on these filters, USCIS receives daily electronic reports, indicating possible fraud leads. Pending applications that may contain evidence of the fraud patterns are called to the attention of USCIS personnel for additional consideration and possible vetting. CIDR provides both a secure and controlled means for FDNS to accomplish this task.

In addition, CIDR's Geospatial Analysis Tool enables CIDR users to normalize address data in and between systems. Legacy information contained in many of USCIS systems was entered manually by individuals, in multiple non-standardized formats. This makes standardized searches across datasets difficult. The Geospatial Analysis Tool standardizes the addresses in and between systems, allowing for a more effective search by location.

Lastly, CIDR users can export data to be further analyzed with third-party tools. These tools allow users to perform comprehensive and flexible searches of USCIS databases that enable CIDR users to visually represent the associative links and connections among data sets and to make connections between data that had previously been unknown.

Identifying Misconduct

The USCIS Office of Special Investigations (OSI), Protective Intelligence Branch (PIB) investigates possible fraud and misuse of immigration information or position by USCIS personnel. CIDR provides OSI with the ability to access information that in the past may have been extremely difficult or impossible to extract from legacy immigration benefit systems. Using audit trails from the source systems, CIDR allows analysts from PIB to discover linkages in which

an employee, either for personal gain or by coercion, may be attempting to manipulate the immigration system. CIDR, therefore, helps to insure employee integrity and, by extension, the integrity of the immigration system.

Internal fraud cases are often referred to OSI via classified channels from other federal agencies when there may be a conflict of interest within their agency's investigation division. As these referrals are classified, the queries of USCIS systems that are related to these investigations are also classified. CIDR is the only tool available to OSI that can provide the information needed at the classification level required.

The process for OSI with respect to PIB cases is as follows:

- USCIS Chief Security Officer (CSO) is alerted to the possibility of internal fraud. This notice can be made from a number of sources, including audits conducted by USCIS's Office of Information Technology, a complaint submitted by a USCIS employee or applicant for immigration benefits, a report from the Office of the Inspector General, a complaint submitted by other DHS components, or information passed to OSI from another federal agency.
- The CSO determines the notice of internal fraud to be valid and requests that the PIB examine the case for indications of potential fraud or misuse.
- Using CIDR's suite of tools, PIB analysts conduct searches and examine the audit trails of the source systems found within CIDR and provide a report of their conclusions to the CSO for action.

Responding to RFIs from the DHS I&A, LE, or the IC based on classified criteria

USCIS routinely receives requests for access to its data when the purpose, source, or content of the request is classified. These classified requests are either from:

- USCIS FDNS for immigration fraud, public safety, or national security investigations, when the administrative investigation leads come from classified sources;
- DHS I&A in the form of a RFI, either from DHS I&A reporting or from the IC;[10] or
- RFIs that are received from other government agencies at the classified level.[11]

[10] Once information from CIDR is incorporated into I&A records, the information will be handled in accordance with DHS/IA-001 Enterprise Records System (ERS), 73 FR 28128 (May 15, 2008).
[11] Prior to disclosure, USCIS reviews responsive USCIS information to ensure that all applicable immigration-specific statutory and regulatory confidentiality provisions are considered.

Currently, CIDR maintains an exact copy of the information contained in CLAIMS 3, obtained from the Service Center Computer Linked Application Information Management System (SCCLAIMS)[12], which is updated on a daily basis.

In future releases, CIDR will also maintain an exact copy of information contained in CLAIMS 3, CLAIMS 4, RAPS, APSS, RNACS, and CIS.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The primary legal authorities supporting the collection of the information used by CIDR and stored in CLAIMS 3, CLAIMS 4, RAPS, APSS, RNACS, CIS, and FDNS-DS come from the Immigration and Nationality Act (INA) (8 U.S.C. § 1101 et seq.). CIDR was created for the following three purposes: (1) to vet USCIS application information for indications of possible immigration fraud and national security concerns; (2) to detect possible fraud and misuse of immigration information or position by USCIS employees, for personal gain or by coercion; and (3) to respond to RFIs from DHS I&A and/or the federal IC and LE community members that are based on classified criteria. The legal authority for each of the three stated purposes is as follows:

1) To vet USCIS application information for indications of possible immigration fraud, public safety, and national security concerns.

INA section 103 (8 U.S.C. § 1103) charges the DHS Secretary with the duty of administering and enforcing all laws relating to the immigration and naturalization of aliens, including ferreting out incidents of immigration fraud, and for ensuring that individuals who pose national security threats are not granted immigration benefits. The DHS Secretary has delegated to the USCIS Director pursuant to Homeland Security Delegation No. 0150.1, the following duties: (1) to administer the immigration laws (as defined in section 101(a)(17) of the INA); (2) investigate alleged civil and criminal violations of the immigration laws, including but not limited to, alleged fraud with respect to applications or determinations within the BCIS [predecessor to USCIS] and make recommendations for prosecutions, or other appropriate action when deemed advisable.

Further, the disclosure of immigration information to members of the intelligence and LE communities is compatible with the purpose for which the information was initially collected, as USCIS has a statutory obligation to ensure that an applicant and/ or beneficiary is admissible in

[12] SCCLAIMS is used rather than CLAIMS 3 for efficiency purposes; SCCLAIMS is an FDNS system and contains the CLAIMS 3 data elements needed to support screening, analysis, and reporting. SCCLAIMS receives a daily refresh of CLAIMS 3 data. *See* DHS/USCIS/PIA-016(a) CLAIMS 3, *available at* www.dhs.gov/privacy, for more information.

accordance with section 245(a)(2) of the INA.[13] Section 245 (a)(2) requires that an alien must be admissible to the United States in order to adjust status to that of a lawful permanent resident. Section 212 of the INA[14] lists several categories of inadmissible aliens. An applicant may be found inadmissible if he or she has been convicted of (or admits to having committed) an offense that constitutes a 'crimes involving moral turpitude,'[15] or has engaged in or is suspected of engaging in terrorist activities.[16] Similarly, section 237 of the INA[17] sets forth the grounds by which an alien can be determined to be removable or deportable, including a conviction of for a crime involving moral turpitude[18] and security and related grounds.[19] Thus, disclosing information to the LE or IC that will enable USCIS to ferret out whether an individual has committed a crime involving moral turpitude or is suspected of engaging in a security or related offense, directly bearing on an individual's eligibility for a requested benefit is compatible with the justification for the initial information capture.

2) *Detect possible fraud and misuse of immigration information or position by USCIS employees, for personal gain or by coercion.*

Section 453 of the Homeland Security Act of 2002, as amended, "Professional Responsibility and Quality Review," provides the Director of USCIS with the authority to conduct investigations of non-criminal allegations of misconduct, corruption, and fraud involving any employee of USCIS that are not subject to investigation by the Inspector General for DHS. Further, Section 454 "Employee Discipline" provides that the Director of USCIS, "notwithstanding any other provision of law, impose disciplinary action, including termination of employment, pursuant to policies and procedures applicable to employees of the Federal Bureau of Investigation, on any employee of the Bureau of Citizenship and Immigration Services who willfully deceives Congress or agency leadership on any matter."

3) *Respond to RFIs from the DHS I&A and/or the federal intelligence and law enforcement community members that are based on classified criteria*.

While USCIS is not a member of the IC, as set forth in Executive Order (EO) 12333[20], as amended, "United States Intelligence Activities," it engages in research of DHS immigration-related information and provides responses to classified RFIs on behalf of DHS I&A, which has

[13] INA § 245(a)(2), 8 U.S.C. § 1255, ("Adjustment of status of non-immigrant to that of person admitted for permanent residence").
[14] *Id*. at § 212. 8 U.S.C. § 1255 ("Inadmissible aliens").
[15] *Id*. at § 212 (a)(2), 8 U.S.C. § 1182 (a)(2) ("Criminal and related grounds").
[16] *Id*., at § 212 (a) (3), 8 U.S.C. § 1182 (a)(3) (" Security and related grounds").
[17] *Id*., at § 237, 8 U.S.C. § 1227 ("General classes of deportable aliens.").
[18] *Id*., at § 237 (a)(2), 8 U.S.C. §1227 (a)(2) ("Criminal offense").
[19] *Id*., at § 237(a)(4), 8 U.S.C. §1227 (a)(4) ("Security and related grounds").
[20] United States Intelligence Activities, Executive Order 12333, Fed. Reg. Vol. 46, No. 59941 (Dec. 04, 1981), as amended, available from https://www.gpo.gov/fdsys/pkg/FR-2008-08-04/pdf/E8-17940.pdf.

been designated as a member of the IC. DHS, under Homeland Security Presidential Directive-6 (HSPD-6), "Integration and Use of Screening Information to Protect Against Terrorism,"[21] and the ''Intelligence Reform and Terrorism Prevention Act of 2004" ("IRPTA")[22], has an obligation to share terrorism-related information. Through the DHS I&A RFI process, DHS is identifying possible terrorism-related information as defined by HSPD-6 and IRPTA and thus meeting its obligations.

CIDR provides USCIS with a platform to perform this mandate in a secure environment.

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

The Citizenship and Immigration Data Repository[23] SORN provides coverage for the CIDR system.

Additionally, the following SORNs provide coverage for CIDR receiving data from several USCIS systems:

- Benefits Information System,[24] covers USCIS's collection, use, maintenance, dissemination, and storage of benefit request information, including case processing and decisional data not included in the A-File;
- Asylum Information and Pre-Screening,[25] covers the collection and use of affirmative asylum applications, applications filed with USCIS for suspension of deportation, special rule cancellation of removal pursuant to the Nicaraguan Adjustment and Central American Relief Act,[26] credible fear screening cases,[27] and reasonable fear[28] screening cases;
- Refugee Case Processing and Security Screening Information,[29] covers the collection and use of refugee applicants, refugee derivatives, and follow-to-join applicants;

[21] Homeland Security Presidential Directive 6 (HSPD-6) (Sept. 2003) available at http://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1174.pdf.
[22] Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-485, 118 Stat. 3638, 3664 (2004), as amended.
[23] DHS/USCIS-012 Citizenship and Immigration Data Repository, 75 FR 54642 (September 8, 2010). Final Rule for Privacy Act Exemptions, 75 FR 81371 (December 28, 2010).
[24] DHS/USCIS-007 Benefits Information System, 81 FR 72069 (Oct. 19, 2016).
[25] DHS/USCIS-010 Asylum Information and Pre-Screening, 80 FR 74781 (Nov. 30, 2015).
[26] *See* Nicaraguan Adjustment and Central American Relief Act, Pub. L. No. 105-100, § 203, 111 Stat. 2193, 2196-200 (1997).
[27] *See* 8 U.S.C. § 1225(b)(1)(B).
[28] *See* 8 CFR § 208.31.
[29] DHS/USCIS–017 Refugee Case Processing and Security Screening Information System of Records, 81 FR 72075 (Oct. 19, 2016).

- Alien File, Index, and National File Tracking System,[30] covers the paper and electronic copy A-File and/or Receipt File, supplemental forms, supplemental evidence, and identity history summaries (formally known as RAP sheets), but does not include all case processing and decisional data;
- Fraud Detection and National Security Records,[31] covers the general collection, use, maintenance, and sharing of records for fraud, public safety, national security, and intelligence purposes.
- General Information Technology Access Account Records System[32] covers the access account records of personnel using the systems.

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

Yes. CIDR received an Interim Authority to Test (IATT) from DHS on May 12, 2009. The old system was decommissioned in April 14, 2015. USCIS will submit all new certification and accreditation paperwork for CIDR. A final Authority to Operate (ATO) will be in place when the system goes live. CIDR will have an ATO prior to any user having access to the system.

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

CIDR does not retain the replicated data sets from the underlying USCIS data systems, to include CLAIMS 3, CLAIMS 4, RAPS, APSS, RNACS, and CIS and the associated audit trails of DHS personnel using the systems. The data supplied by these systems are retained by those systems in accordance with their own retention schedules. CIDR simply mirrors these data sets. Information will be removed from CIDR after it has been removed in the source system.

USCIS is working with NARA to develop a records retention schedule to cover the records retained in CIDR, such as classified background check responses. USCIS proposes to retain background check related records 100 years from the date of birth. The 100-year retention period comes from the length of time USCIS may interact with a customer. Further, retaining the data for this period of time will enable USCIS to fight identity fraud and misappropriation of benefits. This

[30] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (Nov. 21, 2013). The Alien File (A-File), Index, and National File Tracking System of Records is the official record system that contains information regarding the transactions of an individual as he/she passes through the U.S. immigration and inspection process. It may also contain information related to U.S. born citizens and others involved in certain immigration crimes. Final Rule for Privacy Act Exemptions, 78 FR 69983 (November 22, 2013).
[31] DHS/USCIS-006 Fraud Detection and National Security, 77 FR 47411 (August 8, 2012). Final Rule for Privacy Act Exemptions, 74 FR 45084 (August 31, 2009).
[32] DHS/ALL-004 General Information Technology Access Account Records System, 77 FR 70792, (November 27, 2012).

proposed records retention schedule is consistent with the approved NARA Disposition Authority Number DAA-0563-2013-0001-0005.

Records used as part of a benefit determination will be maintained in the Alien File and processed in the respective USCIS case management system. The A-File records are permanent whether hard copy or electronic. USCIS transfers the A-Files to the custody of NARA 100 years after the individual's date of birth. Electronic benefits information is archived and disposed of in accordance with NARA-approved retention schedule for the respective USCIS systems.

CIDR retains a record of the classified search request, the results of the request, and a log of these activities for up to 25 years. These are maintained for a minimum of five years in accordance with Director of Central Intelligence Directive (DCID) 6/3. Classified data will be maintained for the period of time required by the originating classification authority.

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.

There are no forms associated with this collection. However, FDNS may collect data from USCIS applications that are covered by the PRA. See the Benefit Request Intake Process PIA[33] for more information on the various forms that cover the initial collection of information from the individual.

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.

CIDR receives information on individuals whose information is maintained in USCIS source systems, USCIS personnel who accessed the underlying source systems, and federal government employees who submit a RFI or other classified correspondence to USCIS.

Individuals whose information is maintained in CIDR's source systems:

This includes persons who have filed (for themselves or on the behalf of others) applications or petitions for immigration benefits under the INA or who have submitted fee payments or received refunds from such applications or petitions; current, former, and potential

[33] *See* DHS/USCIS/PIA-061 Benefit Request Intake Process, *available at* www.dhs.gov/privacy. See Appendix A for specific forms and associated OMB Control Numbers.

(e.g., fiancé(e)) family members of applicants/petitioners; persons who complete immigration forms for applicants and petitioners (e.g., attorneys, form preparers); and name of applicant's employer.

CIDR will not modify the source data contained in the underlying systems. Information collected about individuals may include, but is not limited to:

Names: first name, last name, middle name, and any aliases of the applicant/requestor, beneficiary, or family members. USCIS also collects names from sponsors, form preparers, attorneys, and designated representatives.

Immigration Status: (e.g., Lawful Permanent Resident, U.S. citizen, or parolee, relating to the benefit applicant/petitioner/requestor, beneficiary, family member, or sponsor).

Travel Information: USCIS collects information on the benefit applicants/petitioners/requestors, beneficiary, or family member's immigration status, immigration status expiration dates, destination in the United States, port of entry,[34] days spent outside the United States, dates of entry, arrival and departure dates, passport number, passport place of issue, passport issue date, passport expiration date, travel document number, travel document country of issue, and travel document expiration date.

Marital Status and History: USCIS collects information regarding current and former marital status (i.e., the marital status of the benefit applicant/requestor or beneficiary, the dates of and place of marriages or terminations, and the reason for termination).

Addresses: Benefit applicants/petitioners/requestors, beneficiaries, family members, sponsors, attorneys, and representatives. For certain benefits, a requestor or beneficiary can provide both a home address and a safe address.[35]

Telephone and Facsimile Numbers: Benefit applicants/petitioners/requestors, beneficiaries, family members, sponsors, household members, attorneys, and representatives.

E-mail Addresses: Benefit requestors, beneficiaries, family members, attorneys, and representatives.

Dates of Birth and Age: Benefit applicants/petitioners, beneficiaries, sponsors, and family members.

Unique Identifying Numbers: USCIS collects Alien Numbers (A-Numbers), Social Security numbers (SSN), USCIS Online Account Numbers, receipt numbers, and other identifying

[34] Travel information is collected from the benefit request form, not from a system-to-system interface with U.S. Customs and Border Protection (CBP).
[35] Benefit requestors may use an alternative mailing address, a "safe address," on their benefit requests. USCIS will use this safe address as the mailing address for all correspondence regarding the victim's immigration relief. Using a safe address protects the victim's privacy and maintains confidentiality.

numbers of benefit requestors, beneficiaries, family members, and sponsors.

Citizenship/Nationality: USCIS collects information on the benefit applicants/petitioners/requestors, beneficiary, or family member's country of citizenship or nationality, and country of birth.

Gender: Benefit applicants/petitioners/requestors, beneficiaries, and family members.

Personal Characteristics: Benefit applicants/petitioners/requestors or beneficiary's hair color, eye color, height, weight, race, and ethnicity.

Information about the attorney, representative, form preparer, or interpreter: Full name, business or organization, mailing address, e-mail address, phone number, fax number, signature, language spoken, relationship to the benefit requestor or beneficiary (if applicable). USCIS also collects Attorney Bar Number or equivalent, Bar Membership, Accreditation Date, Board of Immigration Appeals Representative Accreditation Expiration Date, and Law Practice Restriction Explanation.

Biometrics: Benefit applicants/petitioners/requestors or beneficiary's biometric images such as press-print, photograph, details about those images (e.g., capture date), and signature of benefit requestor, beneficiary, interpreter, and representative.

Card Data: Includes details about cards issued for approved applications such as card serial number, RFID data associated with the Employment Authorization Document and the Permanent Resident Card, production site, production status, and time/date stamp of cards.

Tax and Financial Information: USCIS collects tax identification numbers, and financial information (check information, bank account numbers, credit card numbers (the last four digits only) and other tax and financial information information).

Results of Background, Identity and Security Checks: Date of the background check, whether the check returned any derogatory results, whether those results were resolved, and expiration date of the results.

Certifying Agency Information (if applicable):[36] Information collected about the certifying agency includes agency name, certifying official name, title of certifying official, address, phone, fax, agency type, case status, agency category, case number, FBI Number, or State Identification (SID) Number.

[36] For certain immigration benefits, individuals are required to work with an agency that certifies that the individual "has been helpful, is being helpful, or is likely to be helpful" in the investigation or prosecution of the criminal activity. Certifying agencies include federal, state, or local law enforcement agencies, prosecutors, judges, or other authority that investigates or prosecutes criminal activity. Other agencies such as child protective services, the Equal Employment Opportunity Commission, and the Department of Labor also qualify as certifying agencies since they have criminal investigative jurisdiction within their respective areas of expertise. *See* 8 CFR § 214.14(a)(2).

Medical Information: USCIS collects medical information to establish that an applicant is not inadmissible to the United States on public health grounds, as well as in support of a request for an accommodation during an interview. Such information may indicate alcoholism, declaration of incompetence, or family medical history.

Employment Information: USCIS collects employment information (place and address of employment/occupation, type of work, employer name, length of employment, spouse's employment) in its systems to determine the benefit requestor and beneficiary's eligibility.

Military and Selective Service Information: USCIS collects information evidencing Selective Service registration and military service (e.g., Selective Service number, date of registration, application for military exemption, military branch, willingness to bear arms for the United States of America) in its systems to verify that the benefit requestor or beneficiary has registered with Selective Service as required by law.

Information Regarding Organization Membership or Affiliation: USCIS collects information regarding an applicant's organization memberships and affiliations (organizations, associations, clubs, foundations, parties, societies, or similar groups; communist party membership; totalitarian party membership; terrorist organization membership) in its systems to determine whether the applicant poses a security threat to the United States or individuals or has participated in activities that may disqualify him or her for a requested benefit.

Criminal History or Involvement and Moral Character Issues:[37] USCIS collects information regarding an applicant's criminal history, involvement in criminal activities, and information regarding moral character in its systems to assess whether the applicant meets the standards contained in the INA.

Case Processing Information: USCIS records case processing information such as date USCIS received or filed benefit requests; benefit request status; location of record; other control number when applicable; fee receipt data; status of USCIS appointments and interviews; date of issuance of a notice; and whether the benefit request form was referred to FDNS for review.

Final Decision: Includes a notice to the benefit requestors, beneficiary, and/or the representative on record, approval/denial code, etc.

USCIS personnel who accessed the underlying source system:

CIDR maintains information on USCIS personnel who use CIDR and the underlying USCIS systems included in CIDR, which includes, but is not limited to:

[37] *See* INA § 101(f), § 316(e),and 8 CFR § 316.10

- System audit logs, including the Password Issuance Control System (PICS) Identification Numbers assigned to users of underlying PICS-supported USCIS systems;[38] and

- Records of searches, analyses, correspondence, and outputs generated by USCIS personnel in response to a classified request for USCIS immigrant and non-immigrant data.

If information is responsive to an authorized query, CIDR maintains a copy of the search, the results, information related to the purpose for the request, with whom it was shared, the DHS assigned RFI tracking number, if applicable, and, the FDNS-DS assigned case number or USCIS RFI tracking number, if applicable.

Federal government employees who submit a RFI or other classified correspondence to USCIS:

CIDR does not collect or track specific data elements concerning personnel of other federal agencies; however, the classified correspondence associated with FBI name checks or RFIs is maintained in CIDR in a searchable format. These documents may include contact information of personnel of other federal agencies such as names, agency, title, work addresses, or phone numbers.

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

USCIS DATA SOURCES

In the current release, CIDR maintains information from CLAIMS 3, as described below.

- **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. Information in CLAIMS 3 includes information provided by the individual on the application for a requested immigration benefit, as well as family members, beneficiaries, benefit sponsors, representatives, preparers, and interpreters. The information requested varies and not all forms collect the same information. The system contains information to indicate which steps of the adjudication process have been completed such as, an appointment to submit biometrics for a background check, other pending benefits, and whether the applicant is suspected of fraudulent activity.

  CIDR maintains an exact copy of the information contained in CLAIMS 3, obtained from SCCLAIMS, which is hosted on DHS unclassified networks and updated daily. SCCLAIMS is an FDNS system and contains the CLAIMS 3 data elements needed to support screening, analysis, and reporting. SCCLAIMS receives a daily refresh of

[38] *See* DHS/ICE/PIA-013 Password Issuance and Control System (PICS), *available at* www.dhs.gov/privacy.

CLAIMS 3 data. Daily record updates from SCCLAIMS are copied into an encrypted file. This file is checked for consistency and scanned for viruses before being transferred to CIDR for upload. Only authorized USCIS personnel (to include both federal employees and contractors) copy, transfer, and upload data from SCCLAIMS to CIDR.

In future releases, CIDR will also maintain an exact copy of information contained in the following unclassified systems to be ingested into CIDR and updated/refreshed every twenty-four hours, similar to the process described above for CLAIMS 3.

- **CLAIMS 4** is an electronic case management application tracking and processing system. USCIS uses the system as automated support for the variety of tasks associated with processing and adjudicating N-400, *Applications for Naturalization*. Naturalization is the process by which a foreign citizen or foreign national acquires U.S. citizenship after he or she fulfills the requirements established by Congress in the INA. USCIS personnel responsible for adjudicating and supervising naturalization cases, and USCIS clerks supporting these functions, use CLAIMS 4 to track the naturalization adjudication process from application to granting or denying of the benefit.
- **RAPS** is a comprehensive case management tool that enables USCIS to handle and process applications for asylum, pursuant to Section 208 of the INA and applications for suspension of deportation or special rule cancellation of removal pursuant to Nicaraguan Adjustment and Central American Relief Act (NACARA) § 203 of the INA. DHS officials can use RAPS to verify the status of asylum applicants, asylees, and their dependents, to assist with the verification of an individual's immigration history in the course of a review of visa petitions, and other benefit applications as well.
- **APSS** is a case management system that supports USCIS in the screening of individuals in the expedited removal process and of individuals subject to reinstatement of a final order of removal or an administrative removal order based on a conviction of an aggravated felony to determine whether they have credible fear or reasonable fear as defined by 8 C.F.R. § 208.30 and 8 C.F.R. § 208.31.
- **CIS** is a repository of electronic data that summarizes the history of an immigrant in the adjudication process. In addition, CIS maintains the same information about individuals of interest to the Government for investigative purposes. CIS contains information on the status of benefit requestors seeking immigration benefits, to include: lawful permanent residents, naturalized citizens, U.S. border crossers, aliens who illegally entered the United States, aliens who have been issued employment authorization documents, individuals who petitioned for benefits on behalf of family members, and other individuals subject to the provisions of the INA.

  Additionally, CIDR will maintain an information from the following systems:

- **RNACS** was originally developed to meet the information and case management needs of USCIS staff in Headquarters, Service Centers, and the Field Offices. RNACS now supports USCIS' mission by expediting the completion of naturalization application processing, facilitating the management of the naturalization program, assuring uniformity in processing, supporting status queries on naturalization cases nationwide, and producing integrated management and statistical reports on all naturalization casework. RNACS was developed as an interim system to support naturalization processing in the period between the termination of Naturalization Application Casework System and the deployment of a replacement system (CLAIMS4). In 2013, USCIS decommissioned RNACS. However, eCISCOR acts as a data repository for the decommissioned data.

  CIDR will ingest the legacy RNACS data via a one-time ingest from the eCISCOR repository.

- **FDNS-DS** is the primary screening and case management system used to record requests and case determinations involving benefit fraud, public safety, and national security concerns.

  FDNS-DS data will not be ingested into CIDR; however, CIDR users may manually enter a FDNS-DS case number when recording information as part of tracking responses to RFIs.

For additional information about the information collected, used, and disseminated and maintained in these systems, please visit www.dhs.gov/privacy.

Finally, CIDR contains audit trails of the USCIS IT systems discussed above. OSI utilizes this data to conduct investigations of misuse or abuse of the data systems and to take remedial action to include adverse personnel action and/or additional training as appropriate.

Outside of CIDR, USCIS is implementing a cross-domain solution (CDS), which is a service that facilitates the transfer of unclassified information to higher classified networks. The unified system of dedicated hardware and software authenticates manual or automatic transfer of USCIS information, validates the data, and meets stipulated criteria to move between domains. The criteria laid down for approval of legitimate information for inter-domain transfer is predetermined based on security-approved schemas and antivirus software entrusted with data scan, prior to transfer permission from low to high security domains.

USCIS controls what and when data is transferred by placing it into a file drop zone on the unclassified domain. The CDS then extracts the data, validates, scans, and transfers it to a file drop zone in the classified domain. CIDR then extracts and ingests the data from the file drop zone. The transferred data files are never copied by the CDS, and the CDS only logs "who, when, and what" was transferred from the file headers.

CIDR has the capability to store digital record "pointers" that enable a user to look up records in other classified systems, to include the National Counter Terrorism Center's (NCTC) Terrorist Identities Datamart Environment (TIDE), and associated tracking number or a message trafficking indication number from classified sources.[39] CIDR does not have a direct link to these classified systems or sources, nor is data contained in CIDR shared with systems external to USCIS.

CIDR also maintains classified results of the FBI name checks. In response to the FBI name check USCIS performs, when the FBI identifies concerns that include national security information, the FBI returns a response via classified channels. Currently, USCIS receives the response electronically through the Homeland Security Data Network (HSDN).[40] CIDR has a connection to the email server to be able to receive the responses and capture their associated metadata. USCIS ingests and maintains the associated classified records within CIDR. The classified data is saved in CIDR's data repository and made searchable to CIDR users.

CIDR will house information collected as part of responding to RFIs. CIDR users may manually enter a FDNS-DS case number when recording information as part of tracking responses to RFIs; however, FDNS-DS data will not be ingested into CIDR.

CIDR will maintain audit trails (searches and reports) of USCIS IT systems that may demonstrate misuse or abuse of USCIS data systems by USCIS personnel. OSI utilizes this data to conduct investigations of misuse or abuse of the data systems and to take remedial action to include adverse personnel action or additional training as appropriate. For each report generated, CIDR requires a description of why the user generated the report and what it will be used for. CIDR users record this information into CIDR.

[39] TIDE is the U.S. Government's (USG) central repository of information on international terrorist identities. The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 established NCTC in law, and mandated the Center serve as the "central and shared knowledge bank on known and suspected terrorists and international terror groups." TIDE is that knowledge bank and supports the USG's various terrorist screening systems or "watchlists" and the U.S. Intelligence Community's overall counterterrorism mission. The TIDE database includes, to the extent permitted by law, all information the USG possesses related to the identities of individuals known or appropriately suspected to be or to have been involved in activities constituting, in preparation for, in aid of, or related to terrorism (with the exception of purely domestic terrorism information). This information is available to counterterrorism professionals throughout the Intelligence Community, including the Department of Defense, via the web-based, read-only "TIDE Online."

[40] The Homeland Secure Data Network (HSDN) enables classified information to reach federal agencies that are involved in homeland security missions. HSDN is a classified wide-area network utilized by DHS, DHS Components, and other partners, providing effective interconnections to the intelligence community and federal law enforcement resources. HSDN provides DHS the ability to collect, disseminate, and exchange both tactical and strategic intelligence and other homeland security information up to the SECRET level. HSDN also serves as a consolidated backbone that brings together multiple, legacy SECRET-level classified networks across the DHS enterprise.

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

No.

2.4 Discuss how accuracy of the data is ensured.

CIDR obtains copies of the unclassified data sets from other USCIS systems and is not the original collector. CIDR receives daily updates to ensure that the source information contained in CIDR is current within 24 hours.

With respect to the accuracy of the information obtained from other USCIS systems, USCIS takes a number of steps to ensure the accuracy of information at the point of capture and provides opportunities for individuals to correct or update their information throughout the adjudication process. USCIS provides additional information about this process in the source system PIAs and SORNs.

When CIDR begins receiving data from multiple datasets, for example both CLAIMS 3 and CLAIMS 4, the analyst will manually review information obtained from both systems to ensure that the information is related to the same person before those records are linked within CIDR. If the search returns information from what could potentially be different individuals, the CIDR user will follow USCIS standard operating procedures for alerting the system owner(s) of the possible error. If changes are made to the source system, these changes will be propagated to CIDR via the update process described in Section 2.2.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of over-collection of data, given the number of data sets planned to be ingested into CIDR.

Mitigation: The data sets identified for ingestion into CIDR are meant to provide USCIS personnel with roles in the system a holistic view of a case or subject being researched during the vetting of individuals, responding to RFIs, or investigating possible fraud and misuse of immigration information or position by USCIS personnel. CIDR does not collect new information, but rather replicates existing data collected pursuant to USCIS authorities for the underlying data sets. Storing this data in one system on the classified network negates the need to extract multiple copies of data sets when conducting analysis or responding to classified queries, thereby reducing the risk of making unnecessary copies of the data.

Privacy Risk: There is a risk that information contained in CIDR will not be accurate or current, since CIDR draws or plans to draw upon data contained in other USCIS systems.

Mitigation: CIDR receives daily updates from source systems to ensure it is using the most up-to-date information. As additional data sets are added to CIDR, a process will be implemented to ensure that these systems provide periodic updates to CIDR in a timely and efficient manner.

Privacy Risk: Once datasets beyond CLAIMS 3 are incorporated into CIDR, federated searches across the datasets will lead to a risk that the wrong information will be associated with an individual. For example, the system might retrieve information associated with the wrong individual.

Mitigation: In order to mitigate the issue of wrong information being associated with an individual, a CIDR user reviews all results to ensure the correct information is being linked. If issues arise, the CIDR analyst notifies his or her supervisor, who works with Information Technology owners to identify why information is being incorrectly linked. In addition, the results of searches conducted in CIDR are not used as the sole basis for making a determination about whether to grant or deny and individual a benefit.

Privacy Risk: Similarly, there is a risk that data received from external sources (i.e., FBI Name Check results) may be incorrectly matched to an individual within USCIS' data sets or that the information received may be incomplete or inaccurate.

Mitigation: USCIS has built manual and automated data quality checks into CIDR to ensure that data ingested from external sources is complete, timely, and accurate. Records that are incomplete or missing required information will produce an error message prompting a CIDR user to perform a manual review. All records received from external sources must be reviewed manually by a CIDR user who also confirms the accuracy and validity of the data through visual inspection of the data in comparison to USCIS records. When errors occur, CIDR users will contact the data owner to request correction to records or to request resubmission of incomplete records.

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 developed CIDR, hosted on DHS classified networks, in order to make information from SCCLAIMS available to authorized USCIS personnel for the purposes of:

- Vetting USCIS application information for indications of possible immigration fraud and national security concerns;
- Detecting possible fraud and misuse of immigration information or position by USCIS employees, for personal gain or by coercion;
- Responding to RFIs from DHS I&A or the federal IC and LE community members that are based on classified criteria;

- Enabling authorized USCIS users to more efficiently search multiple USCIS systems from a single entry point; and
- Allowing USCIS to securely conduct searches based on classified parameters as a result of CIDR's position on DHS classified networks.

Use of CIDR for Vetting Purposes

There are occasions when USCIS receives information from other federal partners that is classified. One example is the classified response sent to USCIS by the Federal Bureau of Investigation (FBI) in response to the FBI Name Check, a name-based search of the FBI's CRS and UNI. A positive response to the FBI Name Check means that the FBI has information relating to the subject, which is sent to USCIS via email over the classified network, ingested into, and maintained in CIDR. Within CIDR, users can review the classified response along with the data from the original, unclassified submission. CIDR also contains a robust search capability that allows for searching of the metadata associated with the FBI Name Check results.

Use of CIDR to Respond to Investigatory Leads of USCIS Employees and RFIs

In order to assist with investigating classified investigatory leads on USCIS employees, OSI PIB uses CIDR and its source system audit logs to conduct investigations of possible fraud and misuse of immigration information or position by USCIS personnel. The process for OSI with respect to PIB cases is as follows:

- USCIS CSO is alerted to the possibility of internal fraud. This notice can be made from a number of sources, including but not limited to, audits conducted by USCIS's Office of Information Technology, a complaint submitted by a USCIS employee or applicant for immigration benefits, a report from the Office of the Inspector General, a complaint submitted by other DHS components, or information passed to OSI from another federal agency.
- The CSO determines the notice of internal fraud to be valid and requests that the PIB examine the case for indications of potential fraud or misuse.
- Utilizing CIDR's suite of tools, PIB analysts conduct searches and examine the audit trails of the source systems found within CIDR and provide a report of their conclusions to the CSO for action.

Use of CIDR to Response to RFIs

In order to respond to classified RFIs received from IC and LE partners, USCIS must conduct searches on unclassified data sets whose parameters are classified. To facilitate a more efficient and secure environment in which to conduct these queries and to store their results, USCIS determined that creating mirror copies of its unclassified data sets on the classified side would be

the most appropriate solution. CIDR provides the capability to properly conduct and protect classified searches and maintain detailed audit trails of search activities and results. Copying unclassified data from the unclassified systems to a classified site does not render all this information classified. Only the search parameters and their results are classified. CIDR enables USCIS personnel to perform searches of its non-classified data sets in a classified environment, ensuring that the integrity of the classified RFI process is maintained. Based on the results of the searches performed in CIDR, USCIS produces a response to the RFI, which will include the content of the RFI, information from CIDR that is responsive to the RFI, and any necessary explanations to provide proper context and interpretations of the information provided. These responses contain PII when de-identified or statistical data cannot satisfy the RFI. These responses are produced by USCIS personnel as separate electronic documents and sent to DHS I&A in the same manner that the RFI was received; usually via email over the classified email network.

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.

Yes. Although CIDR is not a data mining system, CIDR provides a suite of analysis tools, including a federated search engine, geospatial analysis tools, and an ability to export data for subsequent analysis, as described below:

Federated Search

CIDR provides a federated web-based search tool that permits users to search all or only a select database(s) found within the system. These searches are person-centric, meaning that, in order to conduct a query, a user must start with a specific data point. For CIDR, a user must have at least one of the following data items in order to initiate a query: A-Number, Last Name, Address, Business Name, or Receipt Number. CIDR users can also search the metatag data fields of FBI name check responses. These fields include: First Name, Last Name, A-Number, Place of Birth, Date of Birth, and Social Security number. Users can also query the text from the FBI name check response for other key words.

Geospatial Analysis Tools

The Geospatial Analysis tool enables CIDR users to normalize address data in and between systems. Legacy information contained in many of USCIS systems was data entered manually by individuals, in multiple non-standardized formats. This makes standardized searches across datasets difficult. The Geospatial Analysis Tool standardizes the addresses in and between systems, allowing for a more effective search by location.

As an example, USCIS receives RFIs from other federal sources seeking information about individuals in certain geographic locations. This tool enables USCIS to more effectively perform responsive searches of USCIS data.

Analytical Software

CIDR users have the capability to export data in conjunction with analytical software to visually represent the associative links and connections uncovered by analysts. These tools allow USCIS personnel to perform comprehensive and flexible searches of USCIS databases that will enable them to visually make connections between data that had previously been unknown.

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

No. Only FDNS and OSI employees within USCIS have direct access to the CIDR system. Information generated from CIDR is shared with IC and LE personnel within DHS for the purpose of investigating violations of customs and immigration laws, as well as possible national security-related threats and plots. Any analytical report from CIDR has the potential to be shared with other authorized DHS components. The information will be shared to the extent that the DHS component has demonstrated a need-to-know and the use for the information falls within that component's respective statutory mission.

Based on a need-to-know, USCIS may share classified analytical reports (not raw data) generated from CIDR with other parts of DHS. DHS I&A receives RFIs from other DHS components, vets the requests, and submits the RFI to USCIS. USCIS provides a response to DHS I&A, and DHS I&A forwards the response to the requestor. For example, requestors may include: the DHS Operations Center, U.S. Immigration and Customs Enforcement (ICE), U.S. Customs and Border Protection (CBP), the DHS Office of Biometric Identity Management (OBIM), and the Transportation Security Agency (TSA). Requestors will only receive the information that they are authorized to receive. USCIS will continue to utilize CLAIMS 3, CLAIMS 4, RAPS, APSS, RNACS, and CIS for non-classified information sharing.

CIDR data is transmitted via the DHS HSDN and the Joint Worldwide Intelligence Communication System (JWICS) network.[41] Information from CIDR is sent to DHS I&A in response to RFIs received from the IC and LE communities. These responses are sent via secure email over these networks, or via secure fax.

[41] The sensitive, compartmented information portion of the Defense Information Systems Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. Also called JWICS. (JP 2-0)

3.4 Privacy Impact Analysis: Related to the Uses of Information

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

Mitigation: All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards such as restricting access to authorized personnel who have a need-to-know. Access to CIDR is granted to only a limited number of USCIS users for mission-related purposes.

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

Mitigation: To ensure the information is used consistently with the purposes of the original collection, USCIS administrators monitor internal and external user logs to ensure users are only accessing information related to their job functions.

Prior to accessing CIDR, each user must sign a user access agreement that outlines the appropriate rules of behavior tailored to CIDR. USCIS implements disciplinary rules as a means to govern the use of the system. USCIS reminds employees accessing the system that the system may be monitored for improper use and illicit activity, and the penalties for non-compliance, through a warning banner that reiterates the appropriate uses of the system. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. This acts as a deterrent to unauthorized activity. Additionally, all USCIS employees are required to complete role-based and adjudicator training prior to accessing CIDR.

Developing CIDR on the DHS classified networks helps ensure accountability for appropriate intelligence and law enforcement access and use of CIDR information. CIDR maintains a log of access to its information, including the contents of the search, and the requesting entity, thereby ensuring appropriate use of its information. Previously, classified searches of unclassified data sets required a cumbersome, manual process that would not allow for the logging of searches. CIDR also employs an aggressive audit trail strategy that goes above and beyond the requirements stated in the Director of Central Intelligence Directive (DCID) 6/3, section 4.B.2.a (4). With CIDR's audit trails, it is possible to determine if system use is consistent with the stated uses. Currently, no other USCIS system is capable of this level of oversight and review.

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.

CIDR does not directly collect information from individuals; rather it uses information collected by CLAIMS 3, and in future releases, CLAIMS 4, RAPS, APSS, RNACS, and CIS, and creates new information (the responses to the RFIs). These systems maintain benefit request forms collected directly from the individuals who apply for USCIS benefits, and these individuals are presented with a Privacy Act Statement, that provides notice to individuals about the collection, USCIS's authority to collect information, the purposes of data collection, routine uses of the information, and the consequences of declining to provide the requested information to USCIS. USCIS benefit request forms also contain a provision in which an applicant authorizes USCIS to release any information received from the applicant as needed to determine eligibility for benefits. Individuals are also notified through notices contained on the benefits applications that their information may be shared for law enforcement purposes or in the interest of national security.

Additionally, individuals receive general notice through this PIA and the CIDR SORN.

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

As previously noted, CIDR does not collect the information directly from the individual. The source systems that feed into CIDR provide notice to the individual that information contained on their benefits applications may be used as needed to determine eligibility for benefits or that his or her information may be shared for law enforcement purposes or in the interest of national security. By submitting benefit request forms to USCIS, applicants have consented to USCIS use of the information submitted for adjudication purposes. Applicants who apply for USCIS benefits have an opportunity and ability to decline to provide information.

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 Act Statement, this PIA, and the associated SORNs. All uses of the information are consistent with these notices.

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.

CIDR does not retain the replicated data sets from the underlying USCIS data systems, to include CLAIMS 3, CLAIMS 4, RAPS, APSS, RNACS, and CIS and the associated audit trails of DHS personnel using the systems. The data supplied by these systems are retained by those systems in accordance with their own retention schedules. CIDR simply mirrors these data sets. Information will be removed from CIDR after it has been removed in the source system.

CIDR is also the system of record to maintain electronic copies of the classified background check results from the FBI. USCIS is working with NARA to develop a records retention schedule to cover the CIDR. USCIS proposes to retain such records 100 years from the date of birth. The 100-year retention period comes from the length of time USCIS may interact with a customer. Further, retaining the data for this period of time will enable USCIS to fight identity fraud and misappropriation of benefits. This proposed records retention schedule is consistent with the approved NARA Disposition Authority Number DAA-0563-2013-0001-0005.

Records used as part of a benefit determination will be maintained in the Alien File and processed in the respective USCIS case management system. The A-File records are permanent whether hard copy or electronic. USCIS transfers the A-Files to the custody of NARA 100 years after the individual's date of birth. Electronic benefits information is archived and disposed of in accordance with NARA-approved retention schedule for the respective USCIS systems.

CIDR retains a record of the classified search request, the results of the request, and a log of these activities for up to 25 years. These are maintained for a minimum of five years in accordance with Director of Central Intelligence Directive (DCID) 6/3. Classified data will be maintained for the period of time required by the originating classification authority.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Retaining information in CIDR for longer than necessary could create the risk of using outdated information for the classified searches of the data sets used by CIDR (currently CLAIMS 3, and in future releases CLAIMS 4, RAPS, APSS, RNACS, and CIS).

Mitigation: The data supplied by these systems are retained by those systems in accordance with their own retention schedules. CIDR simply mirrors these data sets. Information will be removed from CIDR after it has been removed in the source system. Additionally, USCIS is developing a records retention schedule for CIDR that appropriately balances the program's need for the information against risks of unauthorized access. Retention of the classified background check results enables the CIDR program to ensure records relating to FDNS administrative investigations are retained for a period consistent with that of the unclassified investigative file, thus a retention period of 100 years is appropriate.

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.

USCIS only shares analytical reports with DHS I&A. DHS I&A may share these reports with IC and LE personnel that demonstrate a need-to-know in the performance of their missions, including federal, state, tribal, local and foreign law enforcement agencies. Similarly, any responses generated are returned to DHS I&A. CIDR does not share information directly with any organization external to DHS. DHS I&A is responsible for ensuring that information released is done so in accordance with federal and DHS policies.

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

The use of data within CIDR is consistent with the routine uses identified in the respective SORNs for the source systems (e.g., CLAIMS 3, CLAIMS 4, RAPS). In addition, DHS published a SORN covering the information maintained in CIDR that also sets forth routine uses for sharing of this information outside of DHS, including:

Routine Use G - To an appropriate federal, state, tribal, 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, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

Routine Use H - To a federal, state, or local agency, or other appropriate entity or individual, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

As a component of the DHS Intelligence Enterprise, USCIS has a role in interfacing with national elements of the Law Enforcement and Intelligence Communities, as well as coordinating information sharing and collaboration. This sharing is compatible with the above routine uses.

In the case of the I&A, CIDR provides the analytical report to DHS I&A and this information is incorporated into I&A records and will be handled in accordance with the DHS Enterprise Records System SORN, which provides routine uses for the sharing of this information with appropriate intelligence and law enforcement partners.

6.3 Does the project place limitations on re-dissemination?

I&A may share the CIDR information with IC and law enforcement personnel that demonstrate a need-to-know in the performance of their missions, including federal, state, tribal, local and foreign law enforcement agencies.

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

Disclosures outside DHS are made in response to RFIs and managed through the DHS I&A RFI process. Any disclosures made are recorded by DHS I&A and also within CIDR.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information may be delivered to agencies outside of DHS by I&A that do not have a need to know CIDR information.

Mitigation: USCIS mitigates this risk by coordinating requests for national security purposes from external entities through DHS Office of Intelligence and Analysis (I&A) Single Point of Service (SPS).[42] This process ensures that requests are reviewed by appropriate stakeholders, to include privacy, civil liberties, and legal reviews.

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?

DHS exempted CIDR records from general access provisions pursuant to 5 U.S.C. §552a(k) (l) and (2). USCIS reviews each request for information within CIDR to determine whether or not the record within CIDR meets the requirements of the exemptions and, as appropriate, disclose information that does not meet the requirements. This does not prevent the individual from gaining access to his or her records that are found within the original source

[42] *See* DHS/ALL/PIA-044 DHS Single Point of Service Request for Information Management Tool, *available at* www.dhs.gov/privacy, for more information.

system. Persons may seek access to records maintained in the source systems that feed into CIDR, currently CLAIMS 3, and in future releases, CLAIMS 4, RAPS, APSS, RNACS, and CIS.

An individual may gain access to his or her USCIS records by filing a FOIA/PA request. If an individual would like to file a FOIA/PA 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

Further information about FOIA/PA 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?

An individual wishing to contest or amend a record in CIDR must request the correction to the source systems (CLAIMS 3, CLAIMS 4, RAPS, APSS, RNACS, and CIS), as these systems update CIDR on a daily basis. Individuals should submit requests 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. 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.

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 Act Statements, and 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

Privacy Risk: The information requested may be exempt from disclosure under the Privacy Act because information contained within CIDR may contain classified information or law enforcement sensitive information, the release of which could possibly compromise ongoing criminal investigations.

Mitigation: USCIS mitigates this risk by using CIDR only for specific purposes, such as application vetting and to respond to classified requests from DHS I&A and the FDNS program.

USCIS determined that permitting access to this information would not be appropriate and has issued a Final Rule to claim an exemption pursuant to 5 U.S.C. §552a(k) (l) and (2). RFIs that have been generated by other USCIS systems of records and uploaded to CIDR will be processed by obtaining information directly from those systems. This risk is also mitigated in that individuals still have the ability to gain access to and correct, as appropriate, records related to the underlying USCIS systems that feed into CIDR.

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 follows the requirements of the DHS 4300A Sensitive Systems Handbook for information assurance and security and the development of sensitive systems for the CIDR system. Access to CIDR is strictly limited and first requires that a user meet the criteria for access to classified information. CIDR has access controls to distinguish between user and administrator roles, and with CIDR's audit trails, it is possible to determine if system use is consistent with the stated uses. Currently, no other system with USCIS is capable of this level of oversight and review.

CIDR also employs an aggressive audit trail strategy that goes above and beyond the requirements stated in the DCID 6/3, section 4.B.2.a(4). The audit trails in CIDR record, the user ID (if applicable to the event), date/time, and computer name for the following events:

- Log-in/Log-out/Failed log in attempts;
- Each record viewed;
- Each query run;
- Each report viewed;
- Each report printed;
- Daily updates;
- Digital record pointers entered;
- Report information entered;
- System errors generated by CIDR tools;
- Sever errors;
- Network errors associated with CIDR's servers, switches, and storage containers; and

- Backup events.

With CIDR's audit trails, it is possible to determine if system use is consistent with the stated uses. Currently, no other USCIS system is capable of this level of oversight and review.

Per DCID 6/3, audit trails are reviewed by the Information Security System Office (ISSO) every 30 days. Audit trails are maintained for a minimum of 5 years.

In the event USCIS determines that there is a need to expand the scope of CIDR utilization, it will prepare an amendment to this PIA prior to the deployment of any new functionality.

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

The USCIS Information System Security Manager (ISSM) provides initial and annual Computer Security Awareness Training with an online training and testing application. This training addresses protecting sensitive information. After passing the background investigation, every employee that accesses the system must sign a "Rules of Behavior" agreement, which includes protecting sensitive information from disclosure to unauthorized individuals or groups. In addition, all users of the DHS classified networks must undergo yearly national security training and mandatory annual 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?

The primary user groups having access to CIDR are authorized users within USCIS (i.e., FDNS and OSI). An authorized user is a USCIS employee, assigned to work on CIDR, with appropriate clearances to conduct classified searches of USCIS datasets, to review classified background check results, and/or to review incoming RFIs and respond. USCIS manages access to information within CIDR through specific user roles with varying levels of access to search and review information. Most users will have read-only access to CIDR's data to perform searches for a specific purpose consistent with their job duties, as verified by a supervisor. In general, because most of CIDR's data consists of replicated data sets, users will not edit records in CIDR.

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?

Memorandums of Agreement (MOA) and Memorandums of Understanding (MOU) between USCIS and other components of DHS, as well as MOAs and MOUs between USCIS or DHS and other agencies, define information sharing procedures for data maintained by FDNS.

MOAs and MOUs document the requesting agency or component's legal authority to acquire such information, as well as USCIS's permission to share in its use under the legal authority granted. All MOAs and MOUs must be reviewed by the program and all applicable parties.

Responsible Officials

Donald K. Hawkins
Privacy Officer
United States Citizenship and Immigration Service
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