Privacy Impact Assessment
for the

Citizenship & Immigration Data Repository (CIDR)

September 8, 2010

<u>Contact Point</u>
Tim Badger
Chief Technology Coordination Division, Office of Security and Integrity
U.S. Citizenship and Immigration Services
Department of Homeland Security
(202) 272-8000

<u>Reviewing Official</u>
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS) U.S Citizenship and Immigration Services (USCIS) developed the Citizenship Immigration Data Repository (CIDR), hosted on DHS classified networks, in order to make information from multiple USCIS benefits administration systems available for querying by authorized USCIS personnel for the following three purposes: (1) vetting USCIS application information for indications of possible immigration fraud and national security concerns, (2) detecting possible fraud and misuse of immigration information or position by USCIS employees, for personal gain or by coercion, and (3) responding to requests for information (RFIs) from the DHS Office of Intelligence and Analysis (I&A) and/or the federal intelligence and law enforcement community members that are based on classified criteria. In conjunction with this PIA, DHS is issuing a new Privacy Act system of records notice to cover the search parameters and the results of the searches.

Overview

USCIS collects personally identifiable information (PII) directly from and about immigrants and non-immigrants through applications and petitions for the purposes of adjudicating and bestowing immigration benefits. USCIS maintains a number of systems to facilitate these purposes, including: the Computer Linked Application Information Management System (CLAIMS 3), CLAIMS 4, the Refugees, Asylum, and Parole System (RAPS), Asylum Pre-screen System (APSS), Re-engineered Naturalization Application Casework System (RNACS) and Central Index System (CIS). As part of the adjudication process, USCIS personnel carry out a number of steps to ensure that an individual is eligible for a requested benefit. One of these steps is the performance of background checks to make certain that an individual is not attempting to obtain the requested benefit by fraudulent means, has not committed a Crime Involving Moral Turpitude[1], and/or does not pose a public safety threat or a threat to national security.

USCIS developed CIDR, hosted on DHS classified networks, in order to make information from these USCIS systems available to authorized USCIS personnel for the purposes of: (1) vetting USCIS application information for indications of possible immigration fraud and national security concerns, (2) detecting possible fraud and misuse of immigration information or position by USCIS employees, for personal gain or by coercion, and (3) responding to RFI from I&A and/or the federal intelligence and law enforcement community members that are based on classified criteria. CIDR enables authorized USCIS users to more efficiently search multiple USCIS systems from a single entry point, the results of which will be retained in CIDR. CIDR's position on DHS classified networks allows USCIS to securely conduct searches based on classified parameters and searches based on possible fraud and national security concerns.

There are occasions when USCIS receives RFIs through I&A from members of the Intelligence Community (IC) and Law Enforcement (LE) that are classified and or occasions when USCIS receives classified investigatory leads related to one of its employees. In order to assist with classified investigatory leads and/or respond to classified I&A RFIs, 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, DHS 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 will enable 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 will produce 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 will contain PII when de-identified or statistical data cannot satisfy the RFI. These responses will be produced by USCIS personnel as separate electronic documents and sent to I&A in the same manner that the RFI was received; usually via email over the classified email network.

DHS is in the process of implementing components of their Information Sharing Environment (ISE). The DHS ISE includes different architectural options for handling classified searches of information that is maintained on unclassified networks. CIDR is one example in which all the data is replicated from the unclassified network to the classified network. DHS is reviewing other approaches, including federated searches between networks. Appropriate privacy documentation will be completed for all approaches that are finalized.

Section 1.0 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 as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

CIDR-MAINTAINED INFORMATION

CIDR contains information largely maintained in other USCIS systems described below. CIDR will not modify the source data contained in the underlying systems. If information is responsive to an authorized query, CIDR will maintain the following: 1) a copy of the search, 2) the results, 3) information related to the purpose for the request, 4) with whom it was shared, 5) the DHS assigned RFI tracking number, and 5) the Fraud Detection and National Security Data

[1] See Immigration and Nationality Act (INA) § 212 and 237; (8 U.S.C. § 1182 and 1227).

System (FDNS-DS)[2] assigned case number and/or a USCIS RFI tracking number.

CIDR also 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),[3] and associated tracking number or a message trafficking indication number from classified sources. CIDR will not have a direct link to these classified systems or sources, nor will data contained in CIDR be shared with systems external to USCIS.

CIDR will also maintain the Classified Letterhead Memorandum (LHM).[4] The LHM contains the classified responses provided by the FBI in response to USCIS background check requests. Currently, the LHM is sent to USCIS electronically using the Homeland Security Data Network (HSDN). CIDR users will be able to search the metatag data fields of the LHMs. These fields include: First Name, Last Name, A-Number, Place of Birth, Date of Birth, and Social Security Number. In addition, users will be able to query the response text for other key words.

USCIS SYSTEMS SOURCE DATA TO BE INCORPORATED IN CIDR

CIDR receives a mirror copy of CLAIMS 3, which is hosted on DHS unclassified networks and updated daily. In future releases of CIDR, copies of datasets from CLAIMS 4, RAPS, APSS, RNACS, and CIS information, which are also hosted on DHS unclassified networks, will be incorporated and updated once daily. CLAIMS 3, CLAIMS 4, RAPS, APSS, RNACS, and CIS all have current privacy documentation in place covering their use of PII. A description of each IT system that CIDR draws or will draw upon is included below.

The following IT systems are covered by the DHS/USCIS-007 Benefits Information System (BIS) System of Records Notice (73 FR 56596 published on September 29, 2008.

CLAIMS 3 is a case management system containing information used to process all immigration benefits, except naturalization, asylum, and refugee claims. Information in CLAIMS 3 includes information provided by the individual on the application for a requested immigration benefit, and varies depending on the benefit. 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.

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 national acquires U.S. citizenship after he or she fulfills the requirements established by Congress in the Immigration and Nationality Act (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

[2] See Fraud Detection and National Security Data System SORN, 73 FR 48231
[3] For more information see www.nctc.gov/doc/Tide_Fact_Sheet.pdf
[4] The USCIS Background Check Request and Response process is addressed in the Background Check

application to granting or denying of the benefit.

RNACS was originally developed to meet the information and case management needs of USCIS staff in headquarters, service processing centers, and the Citizenship Branches in district and regional 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).

The following systems are covered by DHS/USCIS – 010 Asylum Information and Pre-Screening 75 FR 409 published January 5, 2010.

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 supports the tracking and processing of "Credible Fear" and "Reasonable Fear" cases by Asylum staff. It provides for a prescribed progression of activities from data entry through interview, and the granting or denial of parole. It provides for updates on the establishment of identity, establishment of credible fear claims, mandatory bars, etc.

This IT system is covered by DHS/USCIS – 001 Alien File (A-File) and Central Index System (CIS) 72 FR 1755 published January 16, 2007:

CIS, 72 FR 1755, contains information on the status of 57 million applicants/petitioners seeking immigration benefits, to include: lawful permanent residents, naturalized citizens, U.S. border crossers, aliens who illegally entered the U.S., 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.

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

Finally, CIDR will contain audit trails of the USCIS IT systems discussed above. This data will be utilized by the USCIS Office of Security and Integrity to conduct investigations of

System SORN, 72 FR 31082.

misuse or abuse of the data systems and to take remedial action to include adverse personnel action and/or additional training as appropriate[5]

1.2 What are the sources of the information in the system?

Currently, CIDR maintains an exact copy of information in CLAIMS 3, obtained from the Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR), 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, CIS, the classified LHM Repository, and audit trails of USCIS IT systems that may demonstrate misuse or abuse of USCIS data systems by USCIS personnel. These data sets are described in Section 1.1.

1.3 Why is the information being collected, used, disseminated, or maintained?

USCIS developed CIDR in order to: (1) vet USCIS application information for indications of possible immigration fraud and national security concerns; (2) detect possible fraud and misuse of immigration information or position by USCIS employees, for personal gain or by coercion; and (3) respond to RFIs from I&A and/or the federal intelligence and law enforcement community members that are based on classified criteria. CIDR enables authorized USCIS users to more efficiently search multiple USCIS systems from a single entry point, the results of which will be retained in CIDR. CIDR's position on DHS classified networks allows USCIS to securely conduct searches based on classified parameters, as well as searches based on possible fraud and national security concerns.

1.4 How is the information collected?

The information contained in CIDR is collected from USCIS' unclassified systems (see section 1.1) and updated every twenty-four hours. Daily record updates from USCIS's unclassified systems 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 USCIS unclassified systems to CIDR.

In addition to the copies of the unclassified data sets, CIDR does record (via audit logs) searches and reports that are generated. For each report generated, CIDR requires a description of why the user generated the report and what it will be used for. This information is entered by the USCIS analyst assigned to CIDR.

[5] See DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS) September 29, 2009, 74 FR 49882

1.5 How will the information be checked for accuracy?

CIDR obtains copies of the unclassified data sets from other USCIS system of records 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. Additional information about this process is outlined in the PIAs and SORNs of the source systems.

In instances where CIDR is utilizing data received from multiple datasets, for example both CLAIMS3 and CLAIMS4, the analyst reviews the information from both systems to ensure that the information is related to the same person. If the search returns information from what could potentially be different individuals, the CIDR user will follow USCIS procedure 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 1.4.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The primary legal authorities supporting the collection of the information used by CIDR and stored in CLAIMS 3, CLAIMS 4, RAPS, APSS, RNACS, and CIS come from the INA (8 U.S.C. §1101). 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 the I&A and/or the federal intelligence and law enforcement 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 and national security concern.

The INA (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 these duties to the USCIS Director pursuant to Homeland Security Delegation No. 0150.1, as follows:

(H) Authority under section 103(a)(1) of the INA of 1952, as amended, 8 U.S.C. §1103(a)(1), to administer the immigration laws (as defined in section 101(a)(17) of the INA).

(I) Authority to 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 law enforcement 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 accordance with Section 245(a)(2) of the INA.[6] Section 245 (a)(2) requires that an alien must be admissible to the United States in order to adjust status. Section 212 of the INA[7] defines several categories of inadmissible aliens. An applicant may be found inadmissible if he or she has been convicted of specific crimes set forth in the statute defined as 'Crimes Involving Moral Turpitude,'[8] or has engaged in or is suspected of engaging in terrorist activities.[9] Similarly, Section 237 of the INA[10] sets forth the grounds by which an alien can be determined to be removable or deportable, including the commission of 'Crimes Involving Moral Turpitude'[11] and Security and related grounds.[12] Thus, disclosing information to the law enforcement or intelligence community that will enable USCIS to ferret out whether an individual has committed a 'Crimes 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, and (3) respond to RFIs.

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 the Department. Further, Section 454 "Employee Discipline" provides that the Director of USCIS to, "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 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 Intelligence Community, as set forth in E.O. 12333, 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 been designated as a member of the Intelligence Community.

[6] INA § 245(a)(2), 8 U.S.C. § 1255, ("Adjustment of status of non-immigrant to that of person admitted for permanent residence; record; alien crewmen, aliens continuing or accepting unauthorized employment, and aliens admitted to transit without visa.").
[7] *Id*. at § 212. 8 U.S.C. § 1255 ("Inadmissible aliens").
[8] *Id*. at § 212 (a)(2), 8 U.S.C. § 1182 (a)(2) ("Criminal and related grounds").
[9] *Id*., at § 212 (a) (3), 8 U.S.C. § 1182 (a)(3) (" Security and related grounds").
[10] *Id*., at § 237, 8 U.S.C. § 1227 ("General classes of deportable aliens.").
[11] *Id*., at §237 (a)(2), 8 U.S.C. §1227 (a)(2) ("Criminal offense").
[12] *Id*., at §237(a)(4), 8 U.S.C. §1227 (a)(4) ("Security and related grounds").

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

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

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy Risk: Since CIDR draws or plans to draw upon data contained in other USCIS systems, there is a risk that the information contained in CIDR will not be accurate or current. As such, the possibility exists that erroneous information could be shared with an outside agency or relied upon; resulting in an adverse adjudication of an individual's benefit application.

Mitigation: Regarding the risk of potential inaccuracies, CIDR will receive daily updates from host 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: Similarly, given that CIDR uses source data from another system, there is a possibility that an analyst will find that the source data is inaccurate.

Mitigation: In the event an analyst using CIDR finds that information in one system is not accurate because information has been superseded by other information found in a different system, the program analyst will contact the first data owner to determine how the source information (that is now inaccurate) should be updated.

Privacy Risk: Another privacy risk for CIDR is the potential for unauthorized access to the content, source, and results of classified searches.

Mitigation: In order to mitigate concerns related to unauthorized access to the content, source, and results of classified searches, only those with the requisite security clearance and a need to know will have access. CIDR will reside on specified DHS classified networks only, and user access will be controlled. Authorized users with access to information must possess proper security clearances. CIDR has security access controls and audit processes in place to mitigate the risk of unauthorized access.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used. Tools mentioned in this section are fully explained in section 2.2

2.1 Describe all the uses of information.

USCIS developed CIDR, hosted on DHS classified networks, in order to make information from these USCIS systems available to authorized USCIS personnel for the three purposes discussed below.

(1) Vetting Immigration Applications and Petitions for Indicators of Fraud and National Security Threats

As part of the adjudication process, when an applicant/petitioner applies for a USCIS benefit, a background check is conducted on the individual seeking the benefit. USCIS engages in the following three checks to accomplish the background check: 1) FBI Fingerprint Check - a search of the FBI's Criminal Master File, Integrated Automated Fingerprint Identification System (IAFIS). This search will identify applicants/petitioners who have an arrest record; 2) FBI Name Check - a search of the FBI's Universal Index which consists of administrative, applicant, criminal, personnel, and other files compiled for law enforcement purposes; and 3) TECS Enforcement Name Check is a search of a multi-agency database containing information from 26 different agencies. The information in TECS Enforcement records includes records of known and suspected terrorists, sex offenders, people who are considered public safety risks and other people that may be of interest to the law enforcement community. TECS is also to be used to access National Crime Information Center (NCIC) records on wanted persons, criminal histories, and previous federal inspections.

The Fraud Detection and National Security (FDNS) Office within USCIS is tasked with identifying threats to national security presented by individuals who have applied for immigration benefits, combating benefit fraud, and locating and removing vulnerabilities that compromise the integrity of the legal immigration system. Often, indications of fraud and/or threats to national security will be identified as part of the background checks. Applications that manifest related concerns are forwarded to FDNS officers in the field and to FDNS officers at HQ for vetting and resolution. CIDR will enhance FDNS's capabilities to perform these functions.

CIDR has several key functions. First, it is a collaborative tool that enables multiple users to work on the same case. Thus, if an individual is working a fraud or national security case in one location, a second individual may add information to the case elsewhere in the country. As most FDNS officers are in the field, this will help with case resolution.

Second, CIDR allows USCIS personnel to more efficiently identify national security and fraud concerns by allowing USCIS personnel to review the unclassified applications and the classified background material simultaneously.

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 for the first time to search one system to determine what, if any, immigration benefit a person applied for and received.

Fourth, CIDR will use filters based on existing immigration fraud lead reports to identify basic fraud patterns. These patterns are developed in accordance with FDNS and USCIS policy. Based on these filters, USCIS will receive daily electronic reports, indicating possible fraud leads. Pending applications that may contain evidence of the fraud patterns will be called to the attention of USCIS personnel for additional consideration and possible vetting. Currently, USCIS does not have this capability. CIDR provides both a secure and controlled means for FDNS to accomplish this task.

(2) Internal Fraud Detection and Investigation

The USCIS Office of Security and Integrity (OSI), Protective Intelligence Branch, is tasked with investigating possible fraud and misuse of immigration information or position by USCIS personnel. CIDR will provide 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 will allow analysts from the OSI's Protective Intelligence Branch to discover linkages in which an employee, either for personal gain or by coercion, may be attempting to manipulate the immigration system. CIDR will, therefore, help 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. 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 Protective Intelligence 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 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, or 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 Protective Intelligence branch examine the case for indications of potential fraud or misuse.
- Utilizing CIDR's suite of tools, Protective Intelligence analysts examine the audit trails of the source systems found within CIDR and provide a report of their conclusions to the CSO for action.

(3) Responding to Classified Search Requests from USCIS FDNS and DHS Office of Intelligence and Analysis

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

- USCIS FDNS[13] immigration fraud investigations, where the administrative investigation leads come from classified sources;
- From DHS I&A in the form of an RFI, either from I&A reporting or from the Intelligence Community;[14] or
- From RFIs that are received from other government agencies at the classified level. (Note: prior to disclosure, USCIS reviews responsive USCIS information to ensure that all applicable immigration specific statutory and regulatory confidentiality provisions are considered .)

2.2 What types of tools are used to analyze data and what type of data may be produced?

CIDR provides a suite of analysis tools, including a 1) federated search engine, 2) geospatial analysis tools, 3) an analysis tasking management application (RAID), and 4) I2 interface.

1) Federated Search:

CIDR provides a federated web-based search tool that permits users to search all or only 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.

2) 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 location. This tool will enable USCIS to more effectively perform responsive searches of USCIS data.

3) RAID

RAID is an analysis tasking management application that will help analysts in organizing and sharing information. It will produce a collaborative environment, enabling individuals to

[13] See July 29, 2008 USCIS Fraud Detection and National Security Data System (FDNS-DS) PIA for a description of the FDNS background check and adjudicative process related to immigration applications and petitions (application) with suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns, and cases randomly selected for benefit fraud assessments.

[14] Once information from CIDR is incorporated into I&A records, the information will be handled in accordance with the DHS/IA-001 - Enterprise Records System (ERS) System of Records Notice (73 FR 28128).

work the same cases simultaneously. RAID will assist analysts in identifying links among people, places, businesses, accounts, telephone numbers, and other information available in CIDR.

Included in the RAID application is a suite of tools assisting in the extraction and linking of data from both CIDR and Intelligence Community classified databases. All links are person-centric and require active input from analysts, meaning that RAID does not automatically create links nor does it actively search CIDR for links. Rather, RAID creates links based on the information provided to it by analysts. This information will be a combination of both classified and unclassified sources (see section 1.4).

Finally RAID allows USCIS personnel to aggregate all data that he or she may have captured as part of the vetting process, enabling USCIS personnel to gain a comprehensive understanding of the individual applicant.

4) Analysts Notebook:

CIDR will use Analyst's Notebook to visually represent the associative links and connections uncovered by analysts. Users can visually query the CIDR database. These tools will 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.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

USCIS does not use commercially or publicly available data in CIDR.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Privacy Risk: Once datasets beyond CLAIMS3 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 bring up information on person 1 for two sets of data and person 2 for the third.

Mitigation: In order to mitigate the issue of wrong information being associated with an individual, a USCIS analyst will review all results to ensure the correct information is being linked. If issues arise, the CIDR analysts will work to notify their supervisor, who will work with Information Technology owners to identify why the information is being 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: Risks against unauthorized use of CIDR are mitigated by CIDR's position on DHS classified networks, which requires authorized users to possess proper security clearances. However, there is the additional privacy risk that information originally collected for benefits administration purposes as supplied by CIDR's underlying systems (CLAIMS 3, CLAIMS 4, RAPS, APSS, RNACS, and CIS) may be inappropriately used for law enforcement and intelligence purposes or that the information supplied by CIDR could impact a decision to, for example, grant or deny an individual an immigration benefit.

Mitigation: CIDR has security access controls and audit processes in place to mitigate the risk that personal information will be accessed by unauthorized users and for unauthorized reasons. CIDR users receive computer security and privacy awareness training to mitigate the risk that information will be used inappropriately.

Building CIDR on the DHS classified networks helps ensure accountability for appropriate law enforcement and intelligence use of CIDR information. CIDR will maintain 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.

In addition, the DHS I&A and the USCIS FDNS program have well-established policies and procedures in place for vetting search requests, thereby mitigating the risk of mission/scope creep for CIDR. Further, CIDR makes no decisions regarding the significance of relationships; it simply identifies possible connections for IC and LEO personnel to investigate. The validity of data or relationships identified by CIDR must be verified by the agents/analysts. The risk that incorrect information will be used to make decisions regarding individuals is mitigated by policies requiring IC and LEO personnel to be trained to verify information before including the information in an analytical report, and standard procedures requiring personnel to record the information verification process and findings in their reports.

Privacy Risk: Given the volume of information in CIDR, there is a potential risk that the system could be used for purposes beyond those stated in section 2.1.

Mitigation: Any system has the potential for misuse. CIDR employs several mechanisms to combat this threat. First, training is provided for all users on the use of CIDR. This training is provided on the CIDR website and is required prior to a user gaining access to the system. Users are also reminded of the authorized uses of the system during the log in process via a pop up box, to which users must indicate their understanding of the CIDR uses.

In addition to training, 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). 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
- RAID links established
- 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
- Backup events

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.

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 use, it will prepare an amendment to this PIA prior to the deployment of any new functionality.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Currently, CIDR obtains a copy from CLAIMS 3 and receives daily updates to ensure it has the most up-to-date information. A similar process is envisioned for the use of CLAIMS 4, RAPS, APSS, RNACS, and CIS. Additionally, the audit logs of the systems that have been uploaded will be maintained in CIDR. CIDR will not retain these data sets, but rather, will mirror them. These systems retain their information in accordance with their respective records retention schedules, which are identified in applicable PIAs and SORNS.

CIDR retains a record of the classified search request, the results of the request, and a log of these activities. These are maintained for a minimum of five years in accordance with DCID 6/3.

3.2 How long is information retained?

CIDR does not retain the replicated data sets from CLAIMS 3, CLAIMS 4, RAPS, APSS, RNACS, and CIS. The data supplied by these systems are retained by those systems in accordance with their own retention schedules. CIDR simply mirrors these data sets. Thus, if information is no longer retained in the source system, it will be removed from CIDR at the next update.

CIDR retains a record of the classified search request, the results of the request, and a log of these activities for five years. Classified data will be maintained for the period of time required by the originating classification authority.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

CLAIMS 3, CLAIMS 4, RAPS, APSS, RNACS, and CIS data are retained in accordance with approved NARA records schedules. Data generated by CIDR will be maintained for a minimum of five years in accordance with DCID 6/3.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

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). To mitigate this risk, CIDR receives daily updates from CLAIMS 3 to ensure that queries are conducted upon the most recent information. Retaining the record of the search request, its parameters, and results longer than necessary could also create a risk of unauthorized access.

Mitigation: To mitigate this risk, CIDR has developed a records retention schedule that appropriately balances the program's need for the information against risks of unauthorized access. For example, retention of the audit logs enables the CIDR program to ensure appropriate use of its data, thus a retention period of five years is appropriate. Further, CIDR's position on DHS classified networks provides an additional layer of protection to information retained, in that only authorized individuals with appropriate security clearance may have access to this information.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within DHS.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

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 terrorist 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 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, Immigration and Customs Enforcement (ICE), CBP, U.S. Visitor and Immigrant Status Indicator Technology Program (US-VISIT), and the Transportation Security Agency (TSA). Requestors will only receive the information which they are authorized to receive. USCIS will continue to utilize CLAIMS 3, CLAIMS 4, RAPS, APSS, RNACS, and CIS for non-classified information sharing.

4.2 How is the information transmitted or disclosed?

CIDR data is transmitted via the DHS Homeland Secure Data Network (HSDN) and the Joint Worldwide Intelligence Communication System (JWICS) network. Information from CIDR is sent to DHS I&A in response to RFIs received from the IC and LEO Communities. These responses are sent via secure email over these networks, or via secure fax.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risk: There is a risk that information may be shared with DHS components without a need-to-know.

Mitigation: CIDR uses access controls and audit trails to mitigate the risk that information will be accessed by unauthorized users or improperly used by authorized users. Users receive security and privacy training, and this helps mitigate the risk that information will be used inappropriately. This also mitigates the risk that the information will be provided to individuals without a need-to-know.

Privacy Risk: There is also a risk that personnel from other DHS components will not understand the immigration data and may misinterpret it.

Mitigation: This risk is mitigated by the fact that USCIS is interpreting the data and providing a response to an RFI, rather than just providing the raw data from the underlying systems.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

USCIS shares analytical reports (not raw data) generated from CIDR information with DHS I&A. DHS I&A may share the USCIS CIDR information with intelligence and law enforcement communities personnel that demonstrate a need-to-know in the performance of their missions, including federal, state, tribal, local and foreign law enforcement agencies. All RFIs must come through DHS I&A, where they are vetted to determine whether the requisite authority exists for the request. 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.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The use of CLAIMS 3, CLAIMS 4, and RAPS data for the CIDR is consistent with the routine uses identified in their respective SORNs. In addition, concurrent with this PIA, DHS is publishing a SORN covering the information maintained in CIDR that will also set forth routine uses for sharing of this information outside of the Department. In the case of the Office of Intelligence and Analysis, 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 IC and LE communities.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

DHS I&A is the organization that receives and responds to RFIs from the IC and LE communities. As all of these requests are classified, they are received on classified networks and the responses are sent via secure email on the classified networks.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

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 responding to requests directly from I&A. I&A fully vets all RFIs from the IC and LE communities to ensure that they demonstrate a need-to-know the information in the course of their official duties before they are forwarded on to USCIS.

For RFIs, DHS I&A is responsible for ensuring that information released to external federal, state, local and tribal requestors is in line with federal policies and guidelines.

Privacy Risk: There is also a risk that personnel from other agencies will not understand the immigration data and may misinterpret it.

Mitigation: This risk is mitigated by the fact that USCIS is interpreting the data and providing a response to an RFI so that the appropriate context is provided, rather than just providing the raw data from the underlying systems.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

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 do collect information directly from the individuals who apply for USCIS benefits and these individuals are presented with a Privacy Act Statement, as required by Section (e)(3) of the Privacy Act, and sign a release authorization on the benefit application/petition. The Privacy Act Statement details the authority to collect the information requested and uses to which USCIS will put information the applicant provides on immigration forms and in support of an application. The forms also contain a provision by 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 with law enforcement entities.

This PIA and the SORN DHS is publishing concurrently serve as public notice of the CIDR system, the information it collects and the use of the information contained within the system.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

No. CIDR does not collect information directly from individuals thus opportunities to decline to provide the information do not exist.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No. 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 their information may be shared with law enforcement entities. In most cases, because of the DHS law enforcement, immigration, or intelligence purposes for which CIDR's information is collected, the ability to receive consent is neither appropriate nor feasible.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Applicants for USCIS benefits are made aware that the information they are providing is being collected to determine whether they are eligible for immigration benefits. Each immigration form contains a provision by which an applicant authorizes USCIS to release any information from the application as needed to determine eligibility for benefits. Applicants are also advised that the information provided may be shared with other federal, state, local and foreign law enforcement and regulatory agencies during the course of the investigation.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

As noted in the SORN and the Notice of Proposed Rulemaking (NPRM) for the Privacy Act exemptions, DHS is exempting the records from general access provisions pursuant to 5 U.S.C. §552a (k). Each request for information within CIDR will be reviewed 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 records. 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.

USCIS treats all requests for amendment of information in a system of records as Privacy Act amendment requests. Any individual seeking to access information maintained in CLAIMS 3, CLAIMS 4, RAPS, APSS, RNACS, and CIS and associated systems should direct his or her request to the USCIS FOIA/Privacy Act (PA) Officer at USCIS FOIA/PA, 70 Kimball Avenue, South Burlington, Vermont 05403-6813 (Human resources and procurement records) or USCIS National Records Center (NRC), P. O. Box 648010, Lee's Summit, MO 64064-8010 (all other USCIS records). The process for requesting records can be found at 6 C.F.R. Part 5. Requests for records amendments may also be submitted to the service center where the application was originally submitted. The request should state clearly the information that is being contested, the reasons for contesting it, and the proposed amendment to the information. If USCIS intends to use information that is not contained in the application or supporting documentation (e.g., criminal history received from law enforcement), it will provide formal notice to the applicant and provide them an opportunity to refute the information prior to rendering a final decision regarding the application. This provides yet another mechanism for erroneous information to be corrected.

Requests for access to records in this system must be in writing. Such requests may be submitted by mail or in person. If a request for access is made by mail, the envelope and letter must be clearly marked "Privacy Access Request" to ensure proper and expeditious processing. The requester should provide his or her full name, date and place of birth, and verification of identity (full name, current address, and date and place of birth) in accordance with DHS regulations governing Privacy Act requests (found at 6 C.F.R Part 5), and any other identifying information that may be of assistance in locating the record.

7.2 What are the procedures for correcting inaccurate or erroneous information?

CIDR does not maintain the official DHS record for the source system. Consequently, an individual cannot amend the source record via CIDR. 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 are individuals notified of the procedures for correcting their information?

Privacy Act Statements, including notice of an individual's right to correct information, are also contained in immigration forms published by USCIS. Concurrent with this PIA, DHS is also publishing a SORN covering the maintenance of CIDR. Both the SORN and this PIA provide individuals with notice regarding the procedures for correcting information. This PIA also provides similar notice.

7.4 If no formal redress is provided, what alternatives are available to the individual?

See Section 7.2.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Since any new data generated and/or maintained in CIDR will be exempt from disclosure to individuals under the Privacy Act, individuals may have a limited ability to know about errors that might reside in the systems that feed into CIDR. However, because CIDR is used for application vetting and to respond to classified requests from I&A and the FDNS program, USCIS determined that permitting access to this information would not be appropriate and has filed the necessary Privacy Act documentation to claim an exemption pursuant to 5 U.S.C. §552a (k). RFIs that has been generated by other USCIS systems of records and uploaded to CIDR will be processed by obtaining information directly from those systems. 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 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

The primary user groups having access to CIDR are authorized users within USCIS. An authorized user is a USCIS employee, assigned to work on CIDR, with appropriate clearances to review the classified incoming RFIs and respond.

8.2 Will Department contractors have access to the system?

Contractors will have access to the system, including CIDR developers and information technology operations and maintenance staff. Given that CIDR resides on DHS classified networks, authorized users (contractors and government staff) with access to information must possess proper security clearances. User access to CIDR will be limited as outlined in section 8.1.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

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 .

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

CIDR received its Interim Authority to Test (IATT) from DHS on May 12, 2009. USCIS has submitted all C&A paperwork for CIDR and is awaiting the final Authority to Operate (ATO). CIDR will have an ATO prior to any user having access to the system.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

All queries of CIDR are logged as part of the application’s audit trail. In addition, any report generated from CIDR is logged as well. The audit log includes the user’s name, query or report type, and a time/date stamp. These audit trails are stored for a minimum of five years (see section 1.7).

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The risk that PII will be used inappropriately is mitigated by security training that discusses how to protect sensitive information and by the use of audit mechanisms that log and monitor user activity. The assignment of roles-based usage to establish access requirements based on the user's functions, and regular review of those roles, mitigates the risk that users will be able to access information they are not required to access.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

CIDR is currently a copy of the CLAIMS 3 data set and in future releases will include CLAIMS 4, RAPS, APSS, RNACS, and CIS that resides on classified DHS networks and will provide authorized users the capability to:

- Analyze the information against other classified database systems for reasons of national security and immigration fraud;
- Provide responses to immigration RFIs that are received from other government agencies at the classified level; and
- Provide responses to RFIs in which the subject's name is classified.

9.2 What stage of development is the system in and what project development lifecycle was used?

The CIDR system is developed and its authority to operate is pending.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No, the project does not employ technology that raises privacy concerns that cannot be mitigated (see section 1.7).

Responsible Official

Tim Badger
Chief Technology Coordination Division, Office of Security and Integrity
U.S. Citizenship and Immigration Services

Approval Signature Page

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security