Privacy Impact Assessment
for the

USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum

September 5, 2008

Contact Point
Donald Hawkins, Privacy Officer
United States Citizenship and Immigration Services
Department of Homeland Security
(202) 272-8000

Reviewing Official
John Kropf
Acting Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The United States Citizenship and Immigration Services (USCIS) receives and adjudicates applications for all United States immigration benefits. This PIA covers the USCIS systems associated with processing all immigration benefits except naturalization, asylum, and refugee status. These systems include the Computer Linked Adjudication Information Management System (CLAIMS 3), the Citizenship and Immigration Services Centralized Oracle Repository (CISCOR), the Interim Case Management System (ICMS), Integrated Voice Response System (IVRS), and the Integrated Card Production System (ICPS). Other USCIS systems involved in the processing of benefits are covered by other Privacy Impact Assessments.

Overview

The United States Citizenship and Immigration Services (USCIS) receives and adjudicates petitions and applications for all United States immigration benefits. This PIA covers the USCIS computer systems associated with processing all immigration applications and petitions except naturalization, asylum, and refugee status. These systems include the Computer Linked Adjudication Information Management System (CLAIMS 3), the Citizenship and Immigration Services Centralized Oracle Repository (CISCOR), the Interim Case Management System (ICMS), Integrated Voice Response System (IVRS), and the Integrated Card Production System (ICPS). Other USCIS systems involved in the processing of benefits are covered by other Privacy Impact Assessments.[1]

Immigration Benefit Adjudication Process

The processing and adjudication of an application or petition for immigration benefits or non-immigration benefits (benefit (other than naturalization, asylum, or refugee benefits) occurs in six stages, described below. This PIA covers three of those stages: stage (3) the inputting of information into CLAIMS 3 and associated systems, stage (4) the analysis of the application, and stage (5) the granting or denying of a benefit. Other published USCIS PIAs available on the DHS Privacy Office webpage cover the application receipting and tracking process, biometric collection, background check process, and the fraud detection and national security investigation process.

Stages:

1. Application initiated: The process is initiated when applicant mails (or hand delivers) a completed application, required necessary supporting documents, and applicable fee payment (herein referred to as application) to the address indicated in the DHS application instructions.

2. Receipt of Application: USCIS staff or USCIS contractors record receipt of the application and ensure correct fee payment is received.[2] If the fee payment is correct, USCIS then assigns the applicant an alien number (A-Number) (or matches it with existing A-Number), assigns the application a receipt number, and forwards the application (via hardcopy Alien File [A-File]) or Receipt File to the USCIS National Benefits Center (NBC).[3]

3. Review of Application: NBC staff review the application for completeness[4] and manually input

---

[1] See www.dhs.gov/privacy for a complete listing of USCIS PIAs.
[2] Department of Treasury contractors also perform this function on behalf of USCIS.
[3] If fee payment is incorrect, the application is not accepted and USCIS (/TREAS) sends a notification of incorrect fee payment to the applicant.
[4] If the application is incomplete, the adjudication process is suspended and USCIS notifies the applicant via

the application information into CLAIMS 3 and associated systems. If required, USCIS will schedule an appointment for the applicant to submit biometrics to an Application Support Center (ASC).). NBC then assembles the results of various background checks performed in furtherance of the application, files any hardcopy results of background checks (RAP sheets) into the A-File, and assigns the application to an adjudicator.

4. Adjudication of Application: To begin the substantive analysis of an application, the adjudicators verify the accuracy of the information provided in the application and ascertain the applicant's eligibility for the benefit sought by querying other USCIS and DHS systems. USCIS may also require an in-person interview with the applicant for certain benefits.

5. Granting or Denying Benefits: Based on the results of the adjudication (and interview, if applicable), the adjudicator will deny or grant the benefit.[5] This will result in either a letter denying or granting the benefit. If a benefit is granted, a card will be produced and sent to the applicant.

6. Fraud Detection and National Security: Throughout the application process, adjudicators may refer applications to USCIS fraud detection and national security staff.[6]

System Information Use and Collection

Information in CLAIMS 3 and associated systems includes information provided by the individual on the application for an immigration benefit, and varies depending on the benefit. Additionally, these systems collect 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 3 shares information with many government systems internal and external to DHS. All information sharing is conducted within the parameters of existing Privacy Act of 1974 routine sharing requirements. All sharing is related to the purposes for which the information was originally collected.

The legal authority for CLAIMS 3 is derived from 8 United States Code (U.S.C.) Section 1101 *et seq*. More specifically, 8 U.S.C. Section 1103 charges the Secretary of Department of Homeland Security (DHS) with the duty of administering and enforcing all laws relating to the immigration and naturalization of aliens.

As noted above, this PIA is covering Stages (3), (4), and (5). The following information technology systems support those stages of the adjudication process: the Computer Linked Adjudication Information Management System (CLAIMS 3), the Citizenship and Immigration Services Centralized Oracle Repository (CISCOR), the Interim Case Management System (ICMS), Integrated Voice Response System (IVRS), and the Integrated Card Production System (ICPS).

CLAIMS 3 Functions and Subsystems

CLAIMS 3 includes eight subsystems: (1) Receipt/Data Entry; (2) Adjudication; (3) Notification; (4) Inquiry; (5) Inquiry/Modify; (6) Fee Register; (7) Print Server; and (8) Premium Processing.

---

mail.

[5] If USCIS denies the benefit, it sends the applicant a letter of notification that the benefit was denied and an explanation of why the benefit was denied. If the benefit is granted, the application is forwarded the ICPS to produce the applicable document (Legal Permanent Resident Card, Employment Authorization Document, etc.), which is (mailed? hand-delivered?) to the applicant.

[6] This referral occurs if the adjudicator finds material in the application or the results of criminal background checks that requires analysis by USCIS personnel trained to determine whether the applicant poses a national security threat or is attempting to fraudulently obtain a benefit.

1. The Receipt/Data Entry Subsystem provides tools for data entry and fee collection. It also enables USCIS adjudication officers to review the applications and petitions they rejected and to modify data associated with existing files.
2. The Adjudication Subsystem provides adjudication officers with the capability to process a case (e.g., provides functionality allowing them to approve, deny, revoke, and perform additional evidence request functions).
3. The Notification Subsystem prints notices, modifies address information, prints duplicate notices, prints amended notices, provides case status updates, and prints reports.
4. The Inquiry Subsystem allows users to search CLAIMS 3 record(s) based on a receipt number, A-Number, and an applicant's name or date of birth. The information in this subsystem is read only (users can view data, but cannot change it.)
5. The Inquiry/Modify Subsystem performs the same functions as the Inquiry Subsystem, but the user can make changes. This separate subsystem exists for USCIS personnel who need access to CLAIMS 3 information to perform their job functions and have privileges to change information in the system.
6. The Fee Register Subsystem is run at the end of the day to assist the user in reconciling the total fees receipted by remittance type and by accounting number to facilitate the transmission of the report to the Debt Management Center for the deposit of the fees. The user can request a detailed transaction report by individual user or by office.
7. The Print Server Subsystem allows printing of all types of different notices and reports for internal reporting as well as notifying individuals from CLAIMS 3.
8. The Premium Processing Subsystem allows the user to receive the fee associated with a Request for Premium Processing (form I-907) and collect the pertinent information for premium processing filings. A premium processing fee is a fee paid for expedited treatment of an application.

The Citizenship and Immigration Services Centralized Oracle Repository (CISCOR) is an Oracle database that consolidates the data from USCIS's five CLAIMS 3 service center local area networks (LANs). The CISCOR database is essentially a mirror image of the CLAIMS 3 LAN information and is used for a variety of functions to support CLAIMS 3 adjudications, workflow management, performance measurement, and *ad hoc* queries (e.g., remove the detection and flagging of data errors in the local CLAIMS 3 LAN databases). The CLAIMS 3 information in CISCOR is updated every 15 minutes; thus providing timely CLAIMS 3 information to all USCIS service center users (e.g., persons processing and adjudicating applications) who would otherwise be required to wait for daily CLAIMS 3 Mainframe updates. CISCOR access the service center CLAIMS 3 LAN databases is via a read-only open database connectivity.

Interim Case Management System (ICMS)

Interim Case Management System (ICMS) was created in order to provide CLAIMS 3 LAN system access to the USCIS district offices. ICMS is a web-based application that allows a USCIS district adjudicator to view an application processed in CLAIMS 3, record the adjudication decision, and produce the approval notice and/or documents on line.

Integrated Voice Response System (IVRS)

The Integrated Voice Response System (IVRS) was designed to provide Congressional staff and users who have submitted the Premium Processing Form (I-907) and paid a processing fee with expedited telephone access to certain USCIS CLAIMS 3 case status information (e.g., receipt and form numbers, history action codes [HACs], and USCIS office locations associated with the case). IVRS extracts this

information from CLAIMS 3 and CLAIMS 4 (which is the main system supporting adjudication of naturalization applications) located at the four USCIS CLAIMS service centers. The HACs are derived directly from CLAIMS 3. IVRS provides IVRS end users with particular case status information, such as the date when a certain USCIS form was sent to a particular USCIS location for processing. Prior to 2002, A-Numbers were stored in the IVRS database; however, IVRS no longer collects A-Numbers. A-Numbers stored in IVRS prior to 2002, however, remain in the system. In addition to IVRS, USCIS has developed a user access case status application called the USCIS National Customer Relationship Interface System (CRIS) for which a separate PIA will be published.

Integrated Card Production System (ICPS)

The Integrated Card Production System (ICPS) was developed to allow USCIS to send approved applications that require an official USCIS document/card to the print facility. The cards printed by this facility include the Permanent Resident Card (PRC) (Form I-551) (commonly known as the "Green" Card), the Employment Authorization Document (EAD) (Form I-766), and the State Department B-1/B-2 Visa and Border Crossing Card (Form DSP-150). Names, date of birth, country of birth, and class of admission (refugee etc.) are used to create cards indicating approval of certain immigration benefits granted by USCIS.

These systems throughout the remainder of this PIA will be referred to as *CLAIMS 3 and associated systems* unless the discussion is limited to one or more of the systems covered by this PIA.

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?

CLAIMS 3 and associated systems contain data entered from all CIS customer immigration application forms and petitions except naturalization, refugees and asylum. A complete list of these forms is contained in Appendix A. The information derived from these forms varies and not all forms collect the same information. CLAIMS 3 and associated systems contain the following types of personal data elements for the following purposes:

Names: USCIS collects names (First, Last and Middle) for applicants, petitioners (employer or individual filing for their spouse or children), beneficiaries (worker, dependent, fiancé/spouse, or child), mother's/father's first name and attorneys/representatives to identify the applicant and verify the accuracy of information provided in a petition or application.

Addresses: USCIS collects applicants' addresses, USCIS form preparers, and/or the applicant's attorney/representative in CLAIMS 3 and associated systems. USCIS uses the addresses to send information (e.g., denial, grant and/or requests for additional information) to the applicant or other persons relevant to the immigration process regarding the application. In addition, USCIS collects this information to substantiate an applicant's claim of continuous residence in the U.S. to establish eligibility for benefits.

Telephone Numbers: USCIS collects telephone numbers (applicant's phone number) in certain forms and enters them into CLAIMS 3 and associated systems to contact the applicant or the form preparer if there are questions regarding information contained in the completed forms.

Birth Dates: USCIS collects birth dates (applicant, petitioner, spouse, children/stepchildren/adopted children, fiancé) in certain forms and enters them into in CLAIMS 3 and associated systems to verify the identity of the applicant and to determine his/her eligibility for certain benefits.

Social Security Numbers (SSN): USCIS collects Social Security Numbers (applicant, fiancé, and spouse) in certain forms and enters them into CLAIMS 3 and associated systems in conjunction with other information to verify the identity of the applicant, fiancé and spouse, to determine the applicant's eligibility for certain benefits, and in order to facilitate computer matching activities with the Social Security Administration. For certain applications that involve requests for employment, the SSN is used to verify that the applicant is, in fact, the same person reflected in the employer's records.

Citizenship/Nationality Information: USCIS collects citizenship information (country of nationality, country of citizenship, and country of birth) in certain forms and enters them into CLAIMS 3 and associated systems to determine an applicant's eligibility for certain benefits.

Information Regarding Immigration Status: USCIS collects information regarding immigration (status of current spouse, applicant, and applicant's children, and A-Numbers of applicant's spouse's) and entry to the U.S. (days spent outside the U.S., dates of entry, port of entry, immigration status expiration dates, destination in the U.S.) in certain forms and enters them into CLAIMS 3 and associated systems to determine eligibility for certain benefits.

Marital Status: USCIS collects information regarding marital status (i.e., whether applicant is married, single, widowed or divorced,) in certain forms and enters them into CLAIMS 3 and associated systems to verify the validity of the information provided in a petition or application and to determine the applicant's eligibility for certain benefits sought.

Personal Characteristics: USCIS collects information regarding personal characteristics (hair color, eye color, height, gender, weight) in certain forms and enters them into CLAIMS 3 and associated systems to identify the applicant and to reduce the risk of fraud (e.g., receipt of benefits using someone else's information).

Tax, Financial, and Payment Information: USCIS collects tax identification numbers and Financial/Payment information (check information, bank account numbers, credit card numbers [the last four digits only] and other payment information) in certain forms and enters them into CLAIMS 3 and associated systems to verify the information contained in the application, to ensure compliance with statutory and regulatory requirements, and to determine eligibility for certain benefits sought.

Biometric and Other information Collected to Conduct Background Checks: Title 8 U.S.C. Section 1324a requires criminal history background checks for USCIS applicants. In order to meet the requirements of 8 U.S.C. Section 1324a, USCIS conducts four different background checks on applicants/petitioners applying for certain USCIS benefits (e.g., applications for Permanent Resident status) (1) A Federal Bureau of Investigation (FBI) fingerprint check, (2) a FBI name check, (3) a DHS Customs and Border Protection (CBP) Treasury Enforcement Communication System/Interagency Border Inspection System (TECS/IBIS) name check, and (4) an IDENT fingerprint check.

The only results from any of the four background checks that are stored in CLAIMS 3 and associated systems is the information indicating whether the TECS/IBIS query returned a response indicating that there was no information about the applicant in the TECS/IBIS system. If the TECS/IBIS query returns a response indicating that there is information in the TECS/IBIS system, no notation is made in C3. The authorized TECS/IBIS user will access the system directly to get the detailed information. That detailed information is not systematically stored in any centralized USCIS IT system. A paper copy of the information would be marked "For Official Use Only" and stored in the applicant's paper file.

Results returned to USCIS by IDENT are stored in BBSS, not CLAIMS 3 and associated systems.

If the FBI Fingerprint check response indicates that the person does have a criminal record, the entire RAP sheet is stored in BBSS. USCIS adjudicators access BBSS to view these records in making decisions regarding an applicant's eligibility for USCIS benefits.

The FBI name check response (statement of no hit or a positive hit) is stored in the FBI Query System. The actual information (e.g., RAP sheets or other criminal history information) discovered during the FBI background checks is not stored in CLAIMS 3 and associated systems or the FBI Query System. The actual information discovered is sent by the FBI to USCIS in paper form. The RAP sheet itself is only stored in BBSS. USCIS adjudicators access BBSS to get this information as necessary to process applications.

BBSS and ISRS are being phased out and will soon be replaced by the Biometric Storage System (BSS).[7]

Information Generated by USCIS

CLAIMS 3 and its associated systems noted above contain information regarding the actions of or decisions made by USCIS employees with respect to applications. All data elements in the system are generated from information provided by applicants and USCIS personnel. Information received as part of an interview are maintained in paper copy and are covered by the Alien File (A-File) System of Records Notice (72 FR 1755-59).

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

Most of the information in CLAIMS 3 and associated systems addressed by this PIA come from the data provided by the applicant when he or she completes immigration forms and provides documentation in support of his or her application. Additional information, such as determinations by USCIS personnel about individual applicants and prospective employers, is also recorded in CLAIMS 3 and associated systems.

CLAIMS 3 both sends data to and receives data from a number of different systems and programs. These include other USCIS systems, internal DHS components, and external Federal agencies. Below is an account of how those data exchanges to and from CLAIMS 3 occur for each system.

Internal U.S. Citizenship and Immigration Services (USCIS) Sources

USCIS, Fraud Tracking System (FTS). The USCIS Office of Fraud Detection and National Security (FDNS) developed FTS to decrease fraud in the immigration process. FTS is a case management system used to track and control immigration fraud inquiries and investigative referrals. FTS allows USCIS users to conduct queries of the CLAIMS 3 database on a case-by-case basis to identify potentially fraudulent applications for immigration benefits. When an FDNS Officer identifies suspicious activities either from a tip or by searching the CLAIMS 3 database, a lead is opened in FTS and an FTS identifier is created. The FTS Identifier is a unique system-generated number that is not specifically tied to an individual. This number is not recorded in the CLAIMS 3 system. The inquiry may include investigative reports, administrative inquiry reports, or biographical information on an individual or a group of individuals. It is only after the completion of the inquiry that a note will be made in CLAIMS 3 to record the results of the inquiry. The results of the inquiry are limited to History Action Codes which are 4-digit codes that reveal the status of a particular activity. Depending on the particular case, the HACs would reveal that a finding of fraud was or was not ordered.

[7] See BSS PIA at www.dhs.gov/privacy

USCIS, Marriage Fraud Amendment System (MFAS). MFAS is primarily used to investigate claims of marriage immigration fraud. MFAS supports the processing and control of petitions to remove conditional permanent resident status for alien spouses, sons, and daughters of U.S. citizens or lawful permanent residents. MFAS receives CLAIMS 3 data that allows it to maintain records on eligible immigrant entrants, track cases, generate interview notices, schedule interviews, generate correspondence, and produce management and statistical reports. Specifically, CLAIMS 3 Mainframe sends data on I-751 (Petition to Remove Conditions on Residence) and I-829 forms (Petition by Entrepreneur to Remove Conditions) to MFAS, and receives from MFAS data on whether I-751 and I-829 forms have been approved, denied or are pending.

USCIS Index Cards. CLAIMS 3 collects information from paper index cards containing basic demographic data on individuals regarding cases that were adjudicated prior to the creation of CLAIMS 3, CLAIMS 4, and the USCIS Central Index System (CIS).

USCIS, Central Index System (CIS). CIS supports USCIS records management by collecting, storing, and disseminating biographical and historical information. CIS currently provides information to organizations granting benefits and capturing subsequent immigration status changes; documents chain of custody for enforcement; provides aggregate immigrant statistics and controls, and accounts for record keeping services. Additionally, CIS contains information on the status of over 55 million individuals, including permanent residents, naturalized citizens, border crossers, apprehended aliens, legalized aliens, and aliens issued employment authorization. CIS also contains information regarding individuals who are under investigation (including those who are possible national security threats or threats to the public safety), or who were investigated by the DHS in the past, or who are suspected of violating immigration-related laws or regulations. CLAIMS 3 shares data with CIS in three different ways: 1) CLAIMS 3 sends A-Numbers to CIS. CIS sends back to CLAIMS 3 the A-Number and the name, date of birth, and country of birth associated with that A-Number. CIS then sends the information it has on the A-Number to CLAIMS 3 for verification. (2) CLAIMS 3 sends immigration visa data to CIS when a form I-485, I-181, CR-I89, or OS-155A (see Appendix A for form names) is entered into the system. CLAIMS 3 then sends an update to CIS when there is an approval, denial, or abandonment of an application; and 3) CLAIMS 3 sends Employment Authorization Document (EAD) data from the service centers and the local field offices to CIS.

USCIS, CLAIMS 4. CLAIMS 3 receives information from and sends information to CLAIMS 4 regarding Change of Address forms (Form AR-11) to ensure that both systems are current and accurate.

USCIS, Receipt and Alien-File Accountability and Control System (RAFACS). RAFACS is the file management system in use at USCIS service centers (SCs) and most local offices. The CLAIMS 4 interface with RAFACS allows checks to determine if a particular A-File is present at a processing site. If not, the files are retrieved through CIS transfer requests and cases are held until the files arrive on-site. CLAIMS 4 users are able to query RAFACS for the location of A-Files onsite at any stage of naturalization processing. This interface updates CLAIMS 3 to reflect the receipt of A-Files requested from other sites, so that cases waiting for those files can be released for the scheduling of interviews. RAFACs is currently being phased out and will soon be replaced by the National File Tracking System (NFTS).

USCIS, Private Attorney Maintenance System (PAMS). PAMS contains data on applicants' attorneys such as name, firm, and address. Each attorney is identified by an identification code, consisting of the office code and a sequential number. CLAIMS 3 searches for attorney data, and if the data is not there, sends a request for attorney data to PAMS (for I-687, I-698, and I-694 cases). The CLAIMS 3 Mainframe then receives attorney data confirmation from PAMS.

Internal DHS Sources (Outside USCIS)

The DHS Immigration and Customs Enforcement's (ICE) Student and Exchange Visitor Information System (SEVIS). SEVIS was created by the ICE Student and Exchange Visitor Program (SEVP)

to maintain information on nonimmigrant students and exchange visitors (F, M, and J visas) and their dependents, and also on their associated schools and sponsors. Under the SEVIS process, the nonimmigrant reports to his or her respective school or sponsor and begins participation in the program. The school or sponsor then constantly updates the SEVIS record. If the nonimmigrant no longer qualifies for the benefit sought, for any reason, that information is made available to the ICE Compliance Enforcement Unit in support of investigative action. If the nonimmigrant is eligible for and requests (among other things) reinstatement, a change of status, or employment (i.e. Optional Practical Training [OPT]), a notation of the approval or denial or other status (e.g., pending) of that application is recorded in CLAIMS 3. Via this interface, the CLAIMS 3 Mainframe (MF) also notifies SEVIS when the alien is approved, denied, withdrawn, and in some cases has one of these benefits pending.

DHS CBP TECS/IBIS

After USCIS completes a TECS/IBIS background check search, CLAIMS 3 receives and stores information indicating whether the TECS/IBIS query returned a response indicating that there was no information about the applicant in the TECS/IBIS system. If the TECS/IBIS query returns a response indicating that there is information in the TECS/IBIS system, no notation is made in C3.

CLAIMS 3 also receives immigrant visa issuance and admittance status data (e.g., dates admitted, visa type etc.) from CBP via TECS/IBIS for the purpose of producing cards signifying receipt of certain benefits. CBP receives and uploads to TECS/IBIS this status data from the Department of State Consular Affairs Consolidated Database (CCD) to confirm visa status when visa holders arrive at ports of entry. After the visa holder is admitted at the port of entry, TECS/IBIS sends this data to the appropriate CLAIMS 3 service center. After being admitted, the visa holder fills out an I-89 card on which his or her right index finger print, photograph and signature are affixed. The visa status data are downloaded and the index fingerprint is scanned and downloaded and both entered into CLAIMS 3 at the appropriate USCIS service center and are then sent to ICPS for card production.

External Sources (Outside DHS)

Department of State (DOS). USCIS receives information from the visa portion of the DOS Consular Consolidated Database (CCD) pursuant to an MOU executed in April 2006. The information obtained from CCD includes the history of visa applications and adjudications for subjects who apply for immigration and other benefits. USCIS uses this information to compare CCD visa records with an individual's pending USCIS application to verify the application to ensure consistency. USCIS's use of the information derived from this agreement is limited to the formulation, amendment, administration, and enforcement of immigration and nationality laws. USCIS entered this agreement pursuant to its authority derived from 8 U.S.C. Section 1103. The MOU fully describes the rights and responsibilities of the parties with respect to the information shared, including information security. It also requires updates to ensure data accuracy and training for USCIS users who access the CCD. The visa status is checked against CCD, but no visa status or history is uploaded to CLAIMS 3.

Information obtained from sources other than the applicant is used to verify information provided by the applicants in completed immigration forms and supporting documentation. PII regarding individual CLAIMS 3 users (government personnel and contractors) is also collected to provide accountability if a problem arises with respect to system usage.

CLAIMS 3 and associated systems do not contain information obtained from public websites, data brokers, commercial aggregators and/or other private entities. USCIS obtains information from sources other than the individual applicant (e.g., other USCIS systems) because part of the process supported by CLAIMS 3 and associated systems require the verification of information received from the applicant. The systems themselves do not create a score, analysis or report, but do contain conclusions (i.e., decisions to deny or award of benefits) reached by USCIS system users based on human analysis of applications and

supporting data.

Background Check Processes

FBI Fingerprint Check

The FBI Fingerprint Check is a search of the FBI's Integrated Automated Fingerprint Identification System (IAFIS) to identify applicants who have an arrest record. IAFIS is a national fingerprint and criminal history system maintained by the FBI's Criminal Justice Information Services (CJIS) Division. The applicant's fingerprints are processed by the FBI pursuant to a Memorandum of Understanding between the FBI and USCIS. The fingerprints and biographic data are stored and retained in the FBI system for law enforcement and background check purposes.

FBI Name Check

The FBI Name Check is a search of the FBI's Central Records System (CRS) and Universal Index (UNI). The CRS encompasses the centralized records of FBI Headquarters, FBI field offices, and Legal Attaché offices. The CRS contains FBI investigative, administrative, criminal, personnel, and other files compiled for law enforcement purposes. The UNI consists of administrative, applicant, criminal, personnel, and other law enforcement files. Applicant information (name, date of birth, country of birth, race and gender) is sent to the FBI in order to conduct the name check. The UNI is searched for "main files", files where the name of an individual is the subject of an FBI investigation, and for "reference files." Reference files are files where the name being searched is merely mentioned (not as the main subject) in an investigation. The results of the FBI Name Check ("identification" ["IDENT"] made or "Non-identification" [NON-IDENT"] only) are stored in USCIS' FBI Query system. FBI Query is a mainframe system that stores data related to the activity of the FBI Name Check process. Data is put into FBI Query after the FBI processes the USCIS request. The data in FBI Query includes: Name, Date of Birth, Country of Birth of the applicant, the date the request was sent to the FBI, the date the FBI processed the request, the response from the FBI ("IDENT" or "NON-IDENT"] and, the date the response was loaded into the FBI Query System. The RAP sheet itself is not stored in the FBI Query System.

TECS/IBIS Name Check

The TECS/IBIS Name Check consists of a search of a multi-agency database containing information from 26 different federal agencies. The information in TECS/IBIS includes records of known and suspected terrorists, sex offenders, people who are public safety risks and other individuals that may be of interest (e.g., individuals who have wants and warrants issued against them, people involved in illegal gang activity etc.) to the law enforcement community. The names and dates of birth of CLAIMS 3 applicants are automatically sent to TECS/IBIS electronically by the service center via BBSS. A USCIS user can also log into TECS/IBIS directly and conduct an individual search. If the TECS/IBIS search results indicate that there is no information about that applicant, a "NO HIT" response is forwarded to CLAIMS 3. If the TECS/IBIS search indicates there may be a match, no substantive information is sent to CLAIMS 3. Instead, the user logs directly into TECS/IBIS to get the detailed information. This response data is not currently stored in any centralized USCIS system, but will be stored in the new Background Check Service (BCS) when it becomes operational. TECS/IBIS does not store a record regarding every name that is sent to be queried on the system.

IDENT Fingerprint Check

After a USCIS applicant provides 10 prints and limited biographic data at the ACS, the BBSS server automatically sends the 10 prints and all biographic data collected at the ASC to IDENT.[8] IDENT is a DHS-wide system that stores and processes biometric and biographic information for national security, law enforcement, immigration, intelligence, and other DHS mission-related functions. IDENT is the primary DHS-wide system for the biometric identification and verification of individuals encountered in DHS mission-related processes. The encounter data provides the context of the interaction with an individual, including but not limited to the location of the encounter, document numbers, and/or reason the information was collected. IDENT conducts identification or verification services on behalf of numerous Government (e.g., DHS, Department of State, Department of Justice, and state and local law enforcement) programs that collect biometric and associated biographic data as part of their mission. The information sent to IDENT to conduct queries (10 prints and biographic data) is maintained in the IDENT system to be queried by other IDENT users.

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

USCIS collects this information in order to determine whether to grant immigration benefits to applicants. All information collected from applicants seeking benefits via applications that are processed by CLAIMS 3 and associated systems is necessary to establish the applicant's identity and history with USCIS, as well as eligibility for the benefit sought, and to perform necessary background checks (e.g. to verify statements in an application regarding prior criminal history etc.). USCIS employees enter information into CLAIMS 3 and associated systems to expedite the processing of the application or petition, and to help ensure equitable treatment of applicants, compliance with legislative mandates, and proper implementation of agency policies and regulations.

1.4 How is the information collected?

USCIS collects most of the information in CLAIMS 3 and associated systems directly from the individual applicant via completed immigration forms. A list of the immigration forms from which information is extracted and entered into CLAIMS 3 is contained in Appendix A. USCIS employees enter certain information from these forms into CLAIMS 3. Electronic filing is available for a limited number of forms, which allows USCIS to upload the information from the form directly into CLAIMS 3. Where electronic filing is available, applicants may input information securely via the official USCIS website.

The applicant submits photographs with certain immigration forms. Fingerprints may also be required to complete certain application processes. A completed fingerprint card (form FD-258) is used to fulfill this requirement. The applicant does not submit his or her own fingerprint. USCIS contacts the applicant by mail to inform them of the time and place where their fingerprints will be taken at a specified USCIS ASC.

Process for Collection Biometric and Other information for Background Checks

USCIS collects all 10 of an applicant's fingerprints electronically and also collects biographic data (name, address, date of birth, A-number, SSN [where available]), country of birth, height, weight, eye color, and hair color) at a USCIS Application Support Center (ASC) during certain application processes in

[8] See IDENT PIA at www.dhs.gov/privacy

order to conduct criminal background checks. If an applicant is overseas or otherwise unable to appear at an ASC, fingerprints are taken from hard copy fingerprint cards (FD-258 cards) and are scanned and uploaded to BBSS.

The ASC sends this data via the Biometric Benefits Support System (BBSS) to the service center that received the application that necessitated the background check. The 10 prints and biographic data are encrypted and electronically sent to the FBI where the criminal background checks are conducted.

At the ASCs, USCIS also collects an applicant's digital photograph, right index finger press print, and signature (all three items are collectively referred to as the "image set") if the benefit sought could result in the issuance of a USCIS card (e.g., Permanent Resident Card [PRC], Employment Authorization Document [EAD], Refugee Travel Document or Re-Entry Permit). The image set is then sent to the appropriate USCIS service center via BBSS.

After a USCIS card is produced, the image set and related biographic data are sent from the Integrated Card Production System (ICPS) (which obtains the applicant's name, date of birth, country of birth, and class of admission (refugee etc.) and image sets from CLAIMS 3) to the USCIS Image Storage and Retrieval System (ISRS). Authorized USCIS users can then access ISRS to verify the identity of someone presenting a USCIS issued document.

1.5 How will the information be checked for accuracy?

After receiving applications, USCIS employees place them in receipt files (the application and supporting documentation provided by the applicant) and the applicant's A-file (the record that contains copies of information regarding all transactions involving an individual as he/she passes through the U.S. immigration and inspection process). Standard Operating Procedures (SOPs) include detailed quality control reviews that help to ensure that the data has been accurately entered. These SOPs includes strict procedures for the handling of each different type of application submitted. These procedures ensure that all data fields are completed and describe how data entry personnel must handle inconsistencies and discrepancies in data entries. CLAIMS 3 also deploy software that alerts USCIS data entry personnel when information entered into certain fields is inconsistent (e.g., an address does not match a zip code), and provides instructions for resolving these inconsistencies. The SOPs cover every stage of data entry from the time the envelope containing an application is opened until the time the data is entered and saved in CLAIMS 3.

If upon later review an applicant determines that information in the system is incorrect or outdated (e.g., change of address), the individual may contact the service center where the application was filed and request correction. USCIS treats all requests for corrections as Privacy Act requests. Therefore, such a request triggers the Privacy Act review process to evaluate the accuracy of the information. The accuracy of the data entry can also be challenged during the appeals process if a petition is denied or during the interview process when required.

CLAIMS 3 information is also checked for accuracy through database technical controls, inherent business logic built into the system, and a manual review process (e.g., interviews with the applicants). Improved processes are being put in place for periodic review of PII contained in the system to ensure it is timely, accurate, and relevant as required by the Office of Management and Budget (OMB) and the Privacy Act of 1974. A notification process is also being implemented so that when changes occur (i.e., revisions to PII or the CLAIMS 3 system encounters a major change or is replaced), other resources (e.g., other DHS systems and system users with which/whom information is shared) dependent upon PII contained in this system are alerted.

Finally, if USCIS intends to use criminal history information received during background checks to deny a petition for naturalization, it provides formal notice to the applicant and provides 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.

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

The primary legal authority supporting the collection of the information stored in CLAIMS 3 and associated systems come from 8 U.S.C. Section 1101 *et seq Immigration and Nationality*. More specifically, 8 U.S.C. Section 1103 charges the DHS Secretary with the duty of administering and enforcing all laws relating to the immigration and naturalization of aliens. The DHS Secretary has delegated these duties to the USCIS Under Secretary pursuant to a departmental management directive. In addition, OMB has approved the content and format of every public form used by USCIS.

CLAIMS 3 and affiliated systems contain information that may indicate a person's religious or other organizational affiliation. This information is maintained when it is related to an individual's terms of admission into the United States, such as when an individual's employer is a religious organization, derived from the following subsections of 8 C.F.R. *Aliens and Nationality*:

- § 204.5(m)(2) *Petitions for employment-based immigrants* (m) *Religious Workers*
- § 208.13 *Establishing asylum eligibility*
  § 208.16 *Withholding of removal under section 241(b)(3)(B) of the Act and withholding of removal under the Convention Against Torture*
- § 208.31 *Reasonable fear of persecution or torture determinations involving aliens ordered removed under section 238(b) of the Act and aliens whose removal is reinstated under section 241(a)(5) of the Act.*
- § 212.7(c)(5) 212(e) *Documentary Requirements: Nonimmigrants; Waivers; Admission Of Certain Inadmissible Aliens; Parole* (inadmissibly waiver based on persecution on account of religion)
- § 214.2 *Special requirements for admission, extension, and maintenance of status*
- (p)(3) *Artists, athletes, and entertainers* (claim of culturally unique based on religion)
  (r)(2) *Religious workers*
  245a.32 (and other 245a sections)
- §245(a) *Adjustment Of Status To That Of Persons Admitted For Lawful Temporary Or Permanent Resident Status Under Section 245a Of The Immigration And Nationality Act* (ineligible because of participation in religious persecution)
  §253.1(f) *Parole of Alien Crewmen* (alien crewman paroled because of fear of religious persecution)

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: The primary privacy risk in USCIS data collection is the possibility of data entry errors that might occur when transferring information from forms submitted by applicants into the CLAIMS 3 LAN.

Mitigation: USCIS has mitigated this risk by developing separate, detailed SOPs for handling information collected in each of the numerous USCIS forms completed by applicants. These SOPs include detailed quality control reviews that help to ensure that the information has been accurately transferred from the paper forms submitted by applicants into the CLAIMS 3 LAN. These procedures ensure that all data fields are completed and describe how data entry personnel handle inconsistencies during data entry. The SOPs cover every stage of data entry from the time the envelope is opened until the time the data is entered into CLAIMS 3 and saved.

USCIS also mitigates this risk by allowing applicants to make changes to their information in CLAIMS 3 during the application process. If an applicant later determines that a transcription error occurred during the data input process, the individual may contact the service center where the application was filed and request correction. In addition, USCIS mitigates this risk by accepting some applications electronically in order to remove the possibility of data transcription errors.

Privacy Risk: There is a risk that the owners of a system this large may collect more information that is necessary to perform, the system's necessary functions, thus violating the Privacy Act's data minimization requirements.

Mitigation: USCIS limits the information collected in CLAIMS 3 and associated systems to that necessary to process or adjudicate immigration petitions and applications. Different sets of information are collected for each immigration benefit sought, and this set of information is based on the minimum necessary to process the benefit. In order to minimize the data stored in CLAIMS 3 and associated systems, USCIS limits the PII stored in these systems to information collected from applicants in USCIS forms. All information requested in USCIS forms is necessary to process requests for benefits. All data elements collected were negotiated with and approved by OMB during Paperwork Reduction Act collection reviews. USCIS also disposes of CLAIMS 3 and associated systems' information promptly as required by the records retention schedule negotiated with the National Archives and Records Administration.

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.

2.1 Describe all the uses of information.

USCIS collects and shares the PII discussed in this PIA to establish the applicant's identity and history with USCIS, determine their eligibility for the benefit sought, perform necessary background checks (e.g. to verify criminal history, residence, credit standing, etc.), expedite the processing of the application or petition, help ensure equitable treatment of applicants, compliance with legislative mandates, and proper implementation of agency policies and regulations.

CLAIMS 3 and associated systems use the application data in the following ways.

USCIS Use of Background Check Results Information

Background check result information encompasses data received from the FBI as well as DHS systems (TECS/IBIS and IDENT). This data may include: identifying transactional information (i.e. transaction control number), biographical information, a subject's RAP sheet derived from a fingerprint check, an FBI name check report (containing a brief report outlining the information the FBI has in their files), information from the TECS/IBIS database, and information from the US-VISIT IDENT fingerprint check.

The results of background checks will be used for USCIS benefits adjudication purposes to determine an applicant's eligibility for a benefit. If the background check results from the FBI, TECS/IBIS or IDENT reflect an item of law enforcement or national security interest, USCIS may work with DHS Customs and Border Patrol (CBP), the FBI, or other law enforcement entities, such as Immigration and Customs Enforcement (ICE), to determine if law enforcement actions should be pursued. If the applicant becomes the subject of a national security or law enforcement investigation, the information in CLAIMS 3 and associated systems could be provided to law enforcement agencies in the interest of public safety.

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

USCIS does not use CLAIMS 3 or associated systems to perform complex analytical tasks resulting in, among other types of data matching, relational analysis, scoring, reporting, or pattern analysis. The systems do not make available new or previously unavailable data from newly derived information. USCIS human analysts do, however, collect data from applicants and compare that data to other sources of information to assess whether the applicant is entitled to the benefit sought (see Sections 1.3, 4.0, and 5.1 in this document). Only the outcome of this analysis (i.e., grant or denial of benefits sought) is placed in the applicant's record. Action is only taken with respect to an application based on human analysis and comparisons of applications with data in other systems.

In order to supplement the USCIS SOPs designed to ensure accuracy in the transcription of information from applications to the CLAIMS 3 system, USCIS also deploys a zip code verification function as a technical control designed to ensure accuracy. This program compares the zip code entered into the system with the address entered and alerts the person inputting the data if there is an inconsistency between the two data elements.

DHS has other systems, covered by separate PIAs available on www.dhs.gov/privacy, may use CLAIMS 3 and associated systems' data to conduct analysis, such as the USCIS Fraud Detection and National Security (FDNS) system and the ICE Pattern Analysis and Information Collection (ICEPIC).

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 CLAIMS 3 or associated systems.

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: Individuals who have legitimate access to PII could exceed their authority and use the data for unofficial purposes.

Mitigation: DHS Management Directive System (MD) Number: 11042, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, May 11, 2004, provides guidance for the manner in which DHS employees and contractors must handle Sensitive but Unclassified/For Official Use Only Information in both paper and electronic records (including CLAIMS 3 and associated systems). Additionally, all DHS employees are required to take annual computer security training, which addresses this issue. DHS also maintains rules of behavior for employees who use DHS systems.

USCIS employs SOPs at the service centers to ensure accurate data entry and proper handling and

appropriate use of information. Disciplinary rules are in place to ensure appropriate use of CLAIMS 3 and associated systems information. USCIS also limits access to PII by employing role-based access (only allowing access to users who need particular PII to perform their duties). USCIS also deploys user logs to ensure users are only accessing information related to their job functions.

Section 3.0 Retention

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

3.1 How long is information retained?

Information located in CLAIMS 3 is maintained and disposed of in accordance with the criteria approved by the National Archives and Records Administration (NARA). Information in the master file is destroyed 15 years after the last completed action with respect to the application. System documentation (e.g., manuals) is destroyed when the system is superseded, obsolete, or no longer needed for agency business. Electronic records extracted from immigration benefits applications other than naturalization, asylum, or refugee status completed by applicants is destroyed after the data is transferred to the electronic master file and verified. Daily reports generated by associated information technology systems are maintained for 15 years by the service center that generated the reports and then destroyed.

NARA has determined that ICMS requires no retention schedule because it is an administrative system that contains no data other than the data that is already subject to the CLAIMS 3 retention schedule.

PII is extracted from the immigration forms completed by applicants and entered into CLAIMS 3 and in some cases ICMS. Information in CLAIMS 3 and ICMS is destroyed 15 years after the last completed action with respect to the application. Daily reports generated by CLAIMS 3 are maintained for 15 years by the service center that generated them and then destroyed.

IVRS does not store records. Therefore, it does not require a records retention schedule.

3.2 Has the retention schedule been approved by the component records officer and NARA?

NARA approved the retention schedule for CLAIMS 3 on March 25, 2007. NARA schedules for CISCOR and ICPS are not yet approved but retention schedules have been proposed to NARA.

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

Risk: Keeping data in CLAIMS 3 and associated systems longer than necessary would violate the Fair Information Practice that requires the retention of the minimum amount of information necessary to perform relevant governmental functions.

Mitigation: Although there is always risk inherent in retaining data for any length of time, the CLAIMS 3 and associated systems data retention periods identified in the NARA schedules are consistent with the concept of retaining data only for as long as necessary to support the agency's mission. The schedules proposed and approved by NARA comply with the requirements of the Federal Records Act and

the stated purpose and mission of the systems. The time periods in the NARA schedules were carefully negotiated between USCIS and NARA to ensure that data is retained for the minimum time needed to process the application and make the information available for other USCIS benefits that might be sought by an applicant.

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?

CLAIMS 3 and associated systems exchange data with several systems internal to DHS in order to process applications, as is detailed in Section 1 of this PIA. In addition to those systems previously addressed, CLAIMS 3 is also used to conduct queries for DHS law enforcement intelligence analysts upon request and shares data with the following DHS systems.

Sharing Within U.S. Citizenship and Immigration Services (USCIS)

USCIS, Performance Analysis System (PAS). In order to provide immigration benefit services in a timely manner, USCIS uses the Performance Analysis System on a monthly basis to collect performance data (not PII) on applications received, completed and pending. C3 sends statistical summaries to PAS to assist in this process. The PAS application is a centralized, online, Integrated Data Management System (IDMS) that automates the tracking of G-23 field operations data. These field operations data comprise workload accomplishments and resource expenditures for a wide range of USCIS activities, including examinations, enforcement, and management. PAS allows USCIS users from regional, district, and local field offices to enter, access, and report G-23 (change of attorney form) information that pertains to their office or program area.

USCIS Verification Information System (VIS). VIS is a nationally accessible USCIS database containing selected immigration status information. VIS verifies citizenship and immigration status of individuals seeking government benefits, and allows employers to determine whether a newly hired employee is authorized to work in the United States. VIS directly downloads USCIS CLAIMS 3 change of status and extension of status information on non-citizens and non-immigrants to help determine whether a non-citizen is eligible for any public benefit, license, or credential based on citizenship and immigration status.

USCIS, Refugees, Asylum and Parole System (RAPS). RAPS is the USCIS system in which petitions for asylum and refugee status are processed. CLAIMS 3 sends RAPS updates of applicant address change and employment authorization documents.

USCIS, Nigerian Task Force (NTF). The NTF is a multi-agency task force created to focus on criminal activities of Nigerian crime groups. In 1986, the Senate Permanent Subcommittee on Investigations became concerned about criminal activities of Nigerian crime groups in the U.S. In 1992, Congress appropriated funds to the U.S. Secret Service to establish the Nigerian task force initiative. The Secret Service then established task forces in 13 U.S. cities. These task forces include representatives from USCIS, U.S. Customs Service, U.S. Drug Enforcement Administration, U.S. Postal Inspection Service, Internal Revenue Service, Department of State (DOS), Bureau of Diplomatic Service, banking regulators, and other local, county and state police agencies. In furtherance of this program, USCIS provides Nigerian nationals' applications and petitions to the task force. The CLAIMS 3 Mainframe extracts data from its database to create this file of Nigerian applications and petitions. The file is then transferred by a file transfer protocol (FTP)

process to the appropriate USCIS user.

USCIS, Alien Status Verification Index (ASVI). The system consists of an index of aliens and other persons on whom USCIS has a record as an applicant, petitioner, beneficiary, or possible violator of the Immigration and Nationality Act. ASVI consists of a subset of Central Index System (CIS) data. Extracts are downloaded from CIS (and the CLAIMS 3 Mainframe) to ASVI on a nightly basis. Data elements downloaded include first name, A-Number, date and place of birth, Social Security Number (SSN), date-coded status transaction data and immigration status classification, verification number, and an employment eligibility statement. SSNs are collected because ASVI interacts with the SSA SAVE system to verify that SSA applicants are authorized to do work.

Sharing With Other DHS Components

DHS, Immigration and Custom's Enforcement's (ICE):

Immigration and Customs Enforcement (ICE) Pattern Analysis and Information Collection System (ICEPIC). USCIS shares CLAIMS 3 information with ICE ICEPIC on a case-by-case basis as necessary to support ICE investigations.

ICE Compliance Enforcement Unit (CEU). ICE CEU identifies, locates, and apprehends persons who have violated the terms of their admission to the U.S. USCIS shares CLAIMS 3 information with ICE CEU on a case-by-case basis as necessary to support ICE investigations.

Debt Management Center (DMC). The primary mission of the Debt Management Center (DMC) at DHS is to collect debts resulting from an individual's participation in DHS benefits programs. CLAIMS 3 shares information with the DMC regarding fees charged during various application processes to ensure collection of debts. Through the DMC, CLAIMS 3 and associated systems information may be shared with credit reporting agencies.

Student and Exchange Visitor Information System (SEVIS). SEVIS is the DHS ICE Student and Exchange Visitor Program's (SEVP) system that maintains information on nonimmigrant students and exchange visitors (F, M, and J visas) and their dependents, and also on their associated schools and sponsors. Under the SEVIS process, the nonimmigrant reports to his or her respective school or sponsor and begins participation in the program. At that point, the school or sponsor activates that individual's record in SEVIS by noting that the individual has commenced the program. During the nonimmigrant's stay in the United States, the school or sponsor continuously updates the SEVIS record. If the nonimmigrant falls out of status (i.e., fails to maintain compliance with program requirements) for any reason, that information is made available to the ICE CEU in support of investigative action. If the nonimmigrant is eligible for and requests (among other things) reinstatement, a change of status, or employment (i.e., Optional Practical Training [OPT]), the approval or denial of that application is recorded in CLAIMS 3 and passed to SEVIS to update the individual's record. The CLAIMS 3 Mainframe extracts detailed information from its database for approved, denied, withdrawn, and some pending non-immigrant student case data, and builds a file of transactions to be processed and stored on the SEVIS database. CLAIMS 3 Mainframe notifies SEVIS when the alien student is approved, denied, withdrawn, and in some cases pending for certain benefits.

DHS, United States Visitor and Immigrant Status Indicator Technology Program (US-VISIT)

Arrival and Departure Information System (ADIS). USCIS shares CLAIMS 3 information with the DHS US-VISIT program. DHS established the US-VISIT program to implement an integrated entry and exit data system to record the entry into and exit out of the United States of covered individuals; verify identity; and confirm compliance with the terms of admission to the United States. The US-VISIT program is comprised of multiple systems. One of those systems is US-VISIT's ADIS. ADIS is managed by the US-VISIT program. However, the data in the system is owned by the organization that had the original

authority to collect the data, (e.g., Customs and Border Protection (CBP), which collects the data of individuals who cross the border). ADIS interfaces with CLAIMS 3 for relevant purposes, including status updates regarding benefit adjudication. This sharing is mandated by Section 202 of the Enhanced Border Security and Visa Entry Reform Act of 2002, which required that US-VISIT information be integrated with other DHS databases and data systems. US-VISIT information is separated from CLAIMS 3 data within ADIS. CLAIMS 3 shares the following information with ADIS: Complete name, date of birth, gender, country of birth, nationality, U.S. destination address, passport number, country of issuance, SSN, A-Number, I-94 number, entry date, admission data (current/requested), case status, and Student and Exchange Visitor Information System (SEVIS) ID (current/requested). CLAIMS 3 uses this interface to notify US VISIT (via ADIS) when an alien benefit is pending, approved, or denied.

DHS Intelligence and Analysis (I&A). DHS I&A analysts may access benefits application data for national security purposes.

4.2 How is the information transmitted or disclosed?

All internal sharing is conducted over a secure and reliable DHS electronic interface. This interface utilizes secure network connections on the DHS core network. Paper and electronic records are transported by magnetic tape via secure courier. Federal government employees and their agents must adhere to the OMB guidance provided in OMB Memoranda, M-06-15, *Safeguarding Personally Identifiable Information*, dated May 22, 2006, and M-06-16 *Protection of Sensitive Agency Information*, dated June 23, 2006, setting forth the standards for the handling and safeguarding of personally identifying information. Contractors must also sign non-disclosure agreements that require them to follow departmental transmission and disclosure limitations.

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: The main risk associated with internal information sharing is unauthorized access to PII in CLAIMS 3.

Mitigation: All users must authenticate using a user ID and password in order to access the system. Computer security concerns are minimized by the fact that the information shared internally remains within the DHS environment. Role-based access is used to limit the number of persons who access PII. User access logs track changes to information in the system.

Unauthorized access could also arise during transport of paper and magnetic tape when data is shared internally. This issue is mitigated by the use of a secure courier, and is also being addressed by encryption solutions that will be implemented for magnetic tape during transport to other DHS components.

Privacy Risk: The possibility that users will search for information on individuals and topics beyond the scope of their work is an inherent risk in all systems.

Mitigation: This risk is mitigated by CLAIMS 3 and associated systems training and the enforcement of DHS policies that limit access to all data in CLAIMS 3 and associated systems to ensure it is only used by persons who need it to perform their official functions. An audit trail is also kept for system access and all transactions that request, create, update, or delete information from the system. The audit trail, which includes the date, time, and user for each transaction, is secured from unauthorized modification, access, or destruction. This risk is also mitigated by mandatory annual computer security training.

Privacy Risk: There is a risk that with the sharing of complex sets of data such as that in CLAIMS 3 and associated systems, end users from DHS components who do not have immigration analysis background and training may misinterpret the data.

Mitigation: USCIS is careful to share data with other DHS components who have a need to know, and put the information to a use that is compatible with USCIS SORNs. USCIS trains analysts examining immigration data to understand the data and have professional experience examining that type of data and trusts that other DHS components provide similar training t analysts with similar immigration experience.

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?

CLAIMS 3 and associated systems exchange data with several systems outside of DHS in order to process applications, as is detailed in Section 1 of this PIA. In addition to those systems previously addressed, and in accordance with the Privacy Act of 1974 (as amended) and applicable system of records notice routine uses, USCIS shares select CLAIMS 3 and associated systems information with federal, state, local, tribal, foreign, or international government agencies engaged in national security, law enforcement, immigration, intelligence, and other DHS mission-related functions. USCIS also shares information with the following federal government agencies outside DHS:

External Sharing (Outside DHS)

Department of Justice (DOJ):

Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP). CLAIMS 3 shares information with BJS OJP pursuant to a Memorandum of Understanding (MOU) executed in April 2007. BJA administers the State Criminal Alien Assistance Program (SCAAP) in conjunction with USCIS. SCAAP provides federal funds to states and localities that incurred correctional officer salary costs for incarcerating undocumented criminal aliens with at least one felony or two misdemeanor convictions for violations of state or local law, and incarcerated for at least 4 consecutive days during the reporting period. SCAAP is governed by Section 241(i) of the Immigration and Nationality Act, 8 U.S. Code (U.S.C.) Section 1231(i), as amended, and Title II, Subtitle C, Section 20301, Violent Crime Control and Law Enforcement Act of 1994, Public Law 103-322.

Pursuant to the BJS/USCIS MOU, CLAIMS 3 provides the following data elements to OJP: A-Number, name (first, last, middle), date of birth, unique inmate identifier number, foreign country of birth, date taken into custody, date released from custody, and FBI tracking number. Jurisdictions that submit data to BJA in support of payments for incarceration costs are required to use due diligence to determine the accuracy of the inmate records and related claims submitted to BJA; they may not submit an inmate record if the jurisdiction knows or has reason to know that the information is false or that the inmate does not qualify. OJP examines its undocumented criminal alien data to ensure proper formatting, ensures the completeness of data fields and the eligibility of each entry under the SCAPP program, and provides the results to USCIS in electronic format.

FBI – Russian Nationals. The CLAIMS 3 Mainframe extracts data from its database to create a file on Russian nationals petitioning for non-immigrant worker status. This file is then distributed to the FBI.

USCIS has an existing MOU with the FBI. The terms and conditions for the exchange of data used for fingerprint check purposes are defined in the MOU between USCIS and the FBI. The MOU also limits the use and re-dissemination of the information. The FBI keeps these prints on file for the purpose of conducting fingerprint based background checks for general law enforcement purposes. The prints are stored in the FBI's Civil Electronic File, which is covered in the FBI's Privacy Act Notice for the Fingerprint Identification Record System (FIRS) published on September 28, 1999.

DOS. CLAIMS 3 shares information with the DOS Automated Refugee Tracking System (ARTS). ARTs assists personnel in Department of State posts in processing refugees based on local necessities and requirements. The ARTS database is used to: process eligible cases; send written requests for additional information or informational letters to sponsors and applicants; schedule interviews with USCIS personnel; respond to outside inquiries and take action on requests for case changes; and perform post-interview updates. Form I-765 (Application for Employment Authorization) data is entered into the system by DOS and preprinted form I-94s (Arrival-Departure Record) are generated by DOS from the system. The CLAIMS 3 Mainframe shares information with ARTS for pending, approved, and denied applications and builds a file of transactions to be transmitted to the DOS Non-Immigrant Visa (NIV) server.

An interface between the CLAIMS 3 Mainframe and the DOS NIV provides USCIS Benefits information (i.e. an approved Petition for a Non-Immigrant Worker [form I-129,]) to the DOS DataShare system (DataShare is the name for the DOS Interagency Data Exchange Application [IDEA]). The Datashare system was developed in 1996 as part of a cooperative effort between the former INS, the former U.S. Customs Service, and a number of other interested federal agencies to share immigration benefits information electronically. The purpose of this initiative is to share information regarding persons arriving at our borders, to efficiently produce green cards, and to assist persons who have obtained a USCIS benefit if they have trouble at the border and require confirmation of their status.

CLAIMS 3 tracks aliens who apply to extend their stay in the U.S. As stated in the DOS-USCIS sharing arrangement, the CLAIMS Mainframe notifies DOS when any alien has a benefit pending, or has had a benefit approved, or denied. This interface provides information that is loaded into the Consular Affairs Consolidated Database (CCD) where it is accessible to the DOS systems issuing non-immigrant visas at overseas posts. When retrieved, this data permits consular officers to verify the validity of the I-129 (Petition for a Non-Immigrant Worker) presented to consular posts.

An MOU exists between USCIS and DOS that fully outlines the responsibilities of the parties, including security standards applicable to the information. USCIS provides DOS with electronic read-only access to CLAIMS 3 and 4. Pursuant to this MOU, CLAIMS 3 also provides information to DOS if visa data reviewed by USCIS suggests that a non-U.S. citizen or non-Lawful Permanent Resident might: (1) represent a security threat to the U.S.; or (2) be using false identity or fraudulent documentation. This agreement fully discusses the responsibilities of the parties, including information security, limiting access to the information, training users, and limiting disclosures to third parties.

Social Security Administration (SSA). USCIS shares CLAIMS 3 information with the SSA pursuant to a Computer Matching Agreement (dated June 7, 2007), which allows SSA to determine claim and benefit status under both Title II and Title XVI of the Social Security Act (governing Social Security Retirement, Survivors and Disability Insurance Benefits, and Supplemental Security Income). USCIS provides SSA with an electronic file from the CLAIMS 3 and CLAIMS 4 system of records, which is electronically formatted for transmission to SSA. SSA matches the DHS CLAIMS data with: SSN applicant and holder information maintained in SSA-files. SSA uses the CLAIMS 3 information to determine whether individuals are currently or planning to be absent from the U.S. for more than 30 days because certain persons who are outside the U.S. or similarly lack appropriate statutorily specified residency and citizenship/alienage status are denied Social Security benefits. This agreement has not yet been published in the Federal Register, but when published, it will replace the previous agreement that can be found at 69 Federal Register [FR] 117, at 34214-15 (2004)). The matching operation is carried out under the

authority of Sections 202(n), 1611(f), and 1614(a)(1) of the Social Security Act (42 U.S.C 402(n), 1382(f) and 1382c(a)(1)) and 8 U.S.C. 1611 and 1612 (Aliens and Nationality). Section 1631(e)(1)(B) of the Social Security Act (42 U.S.C. 1383(e)(1)(B)) requires SSA to verify declarations of applicants for and recipients of SSI payments before making a determination of eligibility or payment amount. Section 1631(f) of the Act (42 U.S.C. 1383(f)) requires Federal agencies to provide SSA with information necessary to verify Supplemental Security Income (SSI) eligibility or benefit amounts or to verify other information related to these determinations. In addition, Section 202(n)(2) of the Act specifies that the "Secretary of [the Department of] Homeland Security" notify the Commissioner of Social Security when individuals are deported under specified provisions of Section 237(a) of the Immigration and Nationality Act.

Selective Service System. The Selective Service System is an independent federal agency that is responsible for ensuring emergency military manpower needs pursuant to the Military Selective Service Act (50 U.S.C. App. 451 *et seq.*). Selective Service does not have a direct interface with the CLAIMS 3 system. USCIS extracts information from CLAIMS 3 and creates a file of applicants and petitioners who are eligible for Selective Service registration. This file is then distributed to the Selective Service System on a CD-ROM.

None of this information is directly accessed by agencies outside DHS. It is only provided to the agencies on a case by case basis.

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 current System of Records Notice (SORN) for this system was published in the Federal Register simultaneously with the publication of this PIA. The routine uses, which identify the manner in CLAIMS 3 and associated systems are shared externally, are listed in the SORN. All sharing is compatible with the purpose for which the information was originally requested.

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

Information in CLAIMS 3 and associated systems is tightly controlled and access is granted only to individuals (internally and externally) with a specific need to access the system in order to perform their duties. Each transmission of data from CLAIMS 3 and associated systems to an internal or external system is covered by an Interface Control Document (ICD) that describes the electronic system interface, the levels of authentication and access control that are needed, the data to be shared, and the format and syntax of the data passing through the interface. The ICD also describes the security controls that protect the interface.

None of these external entities has uncontrolled access to the CLAIMS 3 database and associated systems (e.g., external entities have read only access). Once the data is shared, however, the receiving agency is responsible for safeguarding and assuring proper use of the data within its organization. Each of these sharing arrangements is covered by an appropriate routine use in the Benefits Information Systems SORN.

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

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

Mitigation: All external CLAIMS 3 and associated systems sharing arrangements are consistent with existing published routine uses (in the SORN for this system of records) or performed with the consent of the individual whose information is being shared. In all immigration forms processed in CLAIMS 3, applicants are advised that USCIS may provide information from their application to other government agencies. As required by DHS procedures and policies, all CLAIMS 3 and associated systems routine uses and current external sharing arrangements are consistent with the original purpose for which the information was collected.

Information transferred to external agencies that is made part of a system of records is subject to the Privacy Act accuracy, timeliness, relevance and completeness requirements at the receiving agency.

Privacy Risk: The absence of a Memoranda of Understanding (MOU) with the U.S. Selective Service System.

Mitigation: USCIS is in the process of memorializing in writing an MOU with the U.S. Selective Service System with respect to that external sharing arrangement. The MOUs executed between USCIS and other external recipients are discussed in Section 5.1 in the description of each sharing arrangement. These MOUs discuss the parties' respective responsibilities for safeguarding and using the information.

Privacy Risk: There is a risk that with the sharing of complex sets of data such as that in CLAIMS 3 and associated systems, end users from DHS components who do not have immigration analysis background and training may misinterpret the data.

Mitigation: USCIS is careful to share data with external agencies who have a need to know, and put the information to a use that is compatible with USCIS SORNs. USCIS trains analysts examining immigration data to understand the data and have professional experience examining that type of data and trusts that the external agencies provide similar training to analysts with similar immigration experience.

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?

Individuals who apply for USCIS benefits are presented with a Privacy Act Statement as required by Section (e)(3)[9] of the Privacy Act and sign a release authorization on the benefit application/petition. The

[9] The USCIS Privacy Policy can be found at: http://www.uscis.gov and on the instructions that accompany each form.

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. Additionally, USCIS is publishing concurrently with this PIA a system of records notice for Benefits Information System that replaces legacy system of records issued prior to creation of DHS. The following legacy systems will be retired: Justice/INS-013 INS Computer Linked Application Information Management System (CLAIMS) (67 FR 64132 October 17, 2002), Justice/INS-031 Redesigned Naturalization Application Casework System (RNACS) (67 FR 20996 April 29, 2002), and Justice/INS-033 I-551 Renewal Program Temporary Sticker Issuance I-90 Manifest System (SIIMS) (66 FR 6673 January 22, 2001) into one DHS/USCIS system of records notice titled, United States Citizenship and Immigration Services Immigration Application Information System. Categories of individuals, categories of records, and the routine uses of these legacy system of records notices have been consolidated and updated to better reflect DHS/USCIS's immigration application information record systems. This system will be included in the DHS's inventory of record systems.

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

Providing information on immigration forms is a voluntary act on the part of the individual seeking a benefit. The individual, however, must submit a complete application in order to receive USCIS benefits. Applicants may decline to provide the required information; however, it may result in the denial of the applicant's benefit. This condition is clearly stated on each USCIS form.

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

USCIS benefit applications require that applicants provide certain biographic and biometric information that may include submission of fingerprints, photographs, and signatures in addition to other information requested in an application. This information is critical in making an informed adjudication decision to grant or deny a USCIS benefit. The failure to submit such information prohibits USCIS from processing and properly adjudicating the application/petition and thus precludes the applicant from receiving the benefit. Therefore, during the application process, individuals consent to the use of the information submitted for adjudication purposes, including background investigations. Specifically, all USCIS immigration forms include a Privacy Act Statement and require the applicant's signature authorizing "the release of any information from my records that USCIS needs to determine eligibility for the benefit." USCIS forms also contain a statement notifying applicants that their information may be shared with other federal agencies as well. This information is also conveyed in the SORN for this system and in the Privacy Act Statement on the application itself. Applicants are provided an opportunity to review how their information will be used and shared. Individuals grant consent to the collection and use of the information when they sign the application.

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 will be shared with other Federal, state, local and foreign law enforcement and regulatory agencies during the course of the investigation. The SORN provides additional notice to individuals by specifying the routine external uses to which the information will be put. In the USCIS website Privacy Notice,[10] individuals are also notified that electronically submitted information is maintained and destroyed according to the principles of the Federal Records Act, NARA regulations and records schedules, and in some cases may be covered by the Privacy Act and subject to disclosure under the Freedom of Information Act (FOIA). OMB approved all Privacy Act Statements used when collecting data. See the response to Section 1.1 for a discussion of the manner in which USCIS uses CLAIMS 3 and associated systems data.

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?

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 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 Code of Federal Regulations, Section 5.21. 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

[10] Available at http://149.101.23.2/graphics/privnote.htm

(found at 6 Code of Federal Regulations, Section 5.21), 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?

Requests to contest or amend information contained in CLAIMS 3 and associated systems should be submitted 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..

If the particular USCIS process requires a personal interview by a USCIS examiner in order to adjudicate a benefit application, the applicant also has the opportunity to make changes during the interview.

7.3 How are individuals notified of the procedures for correcting their information?

The Privacy Act SORN for this system provides individuals with guidance regarding the procedures for correcting information. This PIA also provides similar notice. Privacy Act Statements, including notice of an individual's right to correct information, are also contained in immigration forms published by USCIS.

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

Applicants are provided opportunity for redress as discussed above.

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

Risk: The main risk with respect to redress is that the right may be limited by Privacy Act exemptions or limited avenues for seeking redress.

Mitigation: The redress and access measures offered by USCIS are appropriate given the purpose of the system. Individuals are given numerous opportunities during and after the completion of the applications process to correct information they have provided and to respond to information received from other sources. USCIS does not claim any Privacy Act access and amendment exemptions for this system so individuals may avail themselves to redress and appeals as stated in the DHS Privacy Act regulations (found at 6 Code of Federal Regulations, Section 5.21).

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?

Because ICMS and the intranet connectivity it provides increase the number of potential USCIS users who have access to the CLAIMS 3 LAN, USCIS deploys role-based access controls to limit access to only those persons who have a need to know this information in order to perform their duties (e.g., those who previously had access to the corresponding paper files before ICMS was implemented).

In compliance with federal law and regulations, users have access to CLAIMS 3 and associated systems on a need to know basis. This need to know is determined by the individual's current job functions. Users may have read-only access to the information if they have a legitimate need to know as validated by their supervisor and the system owner and have successfully completed all personnel security training requirements. System administrators may have access if they are cleared and have legitimate job functions that would require them to view the information. Developers do not have access to production data except for specially cleared individuals who perform systems data maintenance and reporting tasks. Access privileges (for both internal and external users) are limited by establishing role-based user accounts to minimize access to information that is not needed to perform essential job functions.

A user desiring access must complete a Form G-872A & B, USCIS and End User Application for access. This application states the justification for the level of access being requested. The requestor's supervisor, the system owner, and the USCIS Office of the Chief Information Officer (OCIO) review this request; if approved, the requestor's clearance level is independently confirmed and the user account established.

Criteria, procedures, controls, and responsibilities regarding CLAIMS 3 access are contained in the Sensitive System Security plan for CLAIMS 3. Additionally, there are several department and government-wide regulations and directives that provide additional guidance and direction.

8.2 Will Department contractors have access to the system?

Contractors maintain the CLAIMS 3 Mainframe, LAN applications, and associated systems under the direction of the USCIS Office of Information Technology (OIT). Access is provided to contractors only as needed to perform their duties as required in the agreement between USCIS and the contractor and as limited by relevant SOPs. In addition, USCIS employees and contractors who have completed a G-872A & B form (see Section 8.4) and granted appropriate access levels by a supervisor are assigned a login and password to access the system. These users must undergo federally approved clearance investigations and sign appropriate documentation in order to obtain the appropriate access levels.

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

USCIS provides training to all CLAIMS 3 and associated systems users. This training addresses appropriate privacy concerns, including Privacy Act obligations (e.g., SORNs, Privacy Act Statements, etc.). Each USCIS site has the responsibility to ensure that all federal employees and contractors receive the

required annual computer security awareness training and Privacy Act training.

8.4 Has Certification & Accreditation (C&A) been completed for the system or systems supporting the program?

In July of 2008, the CLAIMS 3 LAN obtained a three year Authority to Operate (ATO) from the USCIS CIO after completing DHS C&A requirements. The USCIS OCIO granted the ATO upon due consideration of the findings and recommendations contained in the independent Security Evaluation Report and the recommendations of the USCIS Information System Security Officer (ISSO). The Computer Security Assessment contained an in-depth risk assessment, security plan, contingency plan, and System Test and Evaluation (ST&E), all of which assure compliance with federal IT security requirements. CLAIMS 3 has been classified as a "high" system in accordance with the Federal Information Security Management Act (FISMA) and National Institute for Standards and Technology (NIST) requirements. USCIS implements appropriate controls consistent with NIST requirements.

CISCOR and ICMS were granted an Authority to Operate (ATO) in March 2008. ICPS was granted ATO in July of 2008. All systems are secured in accordance with FISMA requirements.

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

When privileges expire, user access is promptly terminated. After termination of employment at USCIS, access privileges are removed as part of the employee exit clearance process (signed by various persons before departure). Many users have legitimate job duties that require them to query the database for record sets meeting certain criteria. This work is performed under supervisory oversight. Each employee is given annual security awareness training that addresses their duties and responsibilities to protect the data. CLAIMS 3 and associated systems also record History Action Codes that provide a record of significant case processing actions including the user ID of the individual performing these actions. Browsing by the general user community is not permitted. In order to reduce the possibility of misuse and inappropriate dissemination of information, DHS security specifications require auditing capabilities that log user activity. All user actions are tracked via audit logs.

CLAIMS 3 service centers are required to follow USCIS application intake SOPs. Corresponding audits ensure that local processes and procedures are consistent across the enterprise. Within CLAIMS 3 and associated systems there are many business rules that ensure data integrity and consistency.

Remote access to CLAIMS 3 and associated systems is only allowed through an encrypted virtual private network (VPN). Access to the VPN is controlled by numerical authentication tokens.

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?

Privacy Risk: Given the scope of the personal information collected in CLAIMS 3 and associated systems, the security of the information on the system is of critical importance. Due to the sensitive nature of this information, there are inherent security risks (e.g., unauthorized access, use and

transmission/sharing) that require mitigation.

Mitigation: Access and security controls have been established to identify and mitigate privacy risks associated with authorized and unauthorized users, namely misuse and inappropriate dissemination of data. Role-based user accounts are used to minimize the number of persons who have access to the system. Audit trails are kept in order to track and identify any unauthorized changes to information in the system. CLAIMS 3 and associated systems have a comprehensive audit trail tracking and maintenance function that stores information on who submits each query, when the query was run, what the response was, who received the response, and when the response was received. Data encryption is employed where appropriate to ensure that only those authorized to view the data may do so and that the data has not been compromised while in transit. Further, CLAIMS 3 and associated systems comply with DHS and FISMA/NIST security requirements, which provide criteria for securing networks, computers, and computer services against attack and unauthorized information dissemination. Each time CLAIMS 3 and associated systems are modified, the security engineers review the proposed changes and if required, perform Security Testing and Evaluation (ST&E) to confirm that the controls work properly. All personnel are required to complete annual online computer security training.

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, Radio Frequency Identification (RFID), biometrics and other technology.

9.1 What type of project is the program or system?

CLAIMS 3 and associated systems are case tracking system.

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

CLAIMS 3 and associated systems are at the operations and maintenance phase of the DHS system development life cycle.

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

CLAIMS 3 and associated systems only contain information related to the application and adjudication of benefits. The systems do not have the technology or the ability to monitor the activities of individuals or groups beyond that required to adjudicate applications and petitions.

In order to conduct background checks, USCIS requires the collection of biometrics (fingerprints) as part of some application processes. Photographs and signatures are also collected where necessary to issue a card signifying receipt of a benefit. The use of all biometrics collected is limited to the purpose for which the information was collected; the processing of immigration petitions and applications.

Approval Signature

Original signed and on file with the DHS Privacy Office.

John W. Kropf
Acting Chief Privacy Officer
Department of Homeland Security

Appendix A

Immigration Forms/OMB Control Numbers

Title	Form Number	OMB Control Number
Notice of Appeal from Decision of Immigration Judge	EOIR26	1125-0002
Notice of Appeal from Decision of District Director	EOIR29	1125-0010
Immigrant Petition for Relative	I130O	1615-0012
Visa Petition for Spouse	I130S	1615-0012
Effective Date for I131 Advanced Parole Approvals Sent to ICPS	I131B	1615-0013
Application for Replacement/Initial Nonimmigrant Arrival-Departure Document	I-102	1615-0079
Petition for a Nonimmigrant Worker	I-129	1615-009
Petition for Nonimmigrant Worker	I129B	1615-009
Petition for Nonimmigrant Worker: FTA	I129BF	1615-009
Petition for Nonimmigrant Worker: H-1, H-2, or H-3	I129H	1615-0009
Petition for Nonimmigrant Worker: H-1, H-2, or H-3 - FTA	I129HF	1615-009
Petition to Employ Intra-Company Transferee	I129L	1615-0010
Petition to Employ Intra-Company Transferee FTA	I129LF	1615-0010
Petition for Alien Fiancé(e)	I-129F	1615-0001
Nonimmigrant Petition Based on Blanket L Petition	I-129S	1615-0010
Petition for Alien Relative	I-130	1615-0012
Application for Travel Document	I-131	1615-0013
Immigrant Petition for Alien Worker	I-140	1615-0015
Application for Advance Permission to Return to Unrelinquished Domicile	I-191	1615-0016
Application for Advance Permission to Enter as a Non-Immigrant	I-192	1615-0017
Application for Waiver for Passport and/or Visa	I-193	1615-0004
Application for Permission to Reapply for Admission into the United States After Deportation or Removal	I-212	1615-0018
Application for Stay of Deportation	I246	1653-0021

Title	Form Number	OMB Control Number
Appeal, Motion to Reopen or Reconsider	I290A	1615-0095
Notice of Appeal to the Board of Immigration Appeals	I290AA	1615-0095
Notice of Appeal to the Board of Immigration Appeals	I290AP	1615-0095
Certified Appeal, Motion to Reopen or Reconsider	I290C	1615-0095
Motion to Reopen or Reconsider	I290M	1615-0095
Notice of Appeal to the Administrative Appeals Office (AAO)	I-290-B	1615-0095
Immigration Bond	I-352	1653-0022
Petition for Amerasian, Widow(er), or Special Immigrant	I-360	1615-0020
Abandonment of Lawful Permanent Residence Status	I-407	CBP
Application for Naturalization	N-400	1615-0052
Application to Register Permanent Residence or Adjust Status	I-485	1615-0023
Supplement A to Form I-485, Adjustment of Status Under Section 245(i)	I-485 Supplement A	1615-0023
Immigrant Petition by Alien Entrepreneur	I-526	1615-0026
Application to Extend/Change Nonimmigrant Status	I-539	1615-0003
Deficiency Notice to Arriving F-1, M-1, or J-1	I-515	1615-0083
Request Determination that Prospective Immigrant Is an Investor	I526O	1615-0026
Application by Foreign Student	I538	CBP
Application to Extend Temporary Stay	I539O	Same as I-539
Premium Processing	I539PP	Same
Application for Asylum and Withholding of Removal	I-589	1615-0067
Petition to Classify Orphan as an Immediate Relative	I-600	1615-0028
Application for Advance Processing of Orphan Petition	I-600A	1615-0028
Application for Waiver of Ground of Excludability	I-601	1615-0029
Application for Waiver of the Foreign Residence Requirement of Section 212(e) of the Immigration and Nationality Act, as amended	I-612	1615-0030
Health and Human Services Statistical Data for Refugee/Asylee Adjusting Status	I-643	1615-0070
Application for Status as a Temporary Resident Under Section 245A	I-687	1615-0090

Title	Form Number	OMB Control Number
of the Immigration and Nationality Act		
Application for Waiver of Grounds of Excludability Under Sections 245A or 210 of the Immigration and Nationality Act	I-690	1615-0032
Notice of Appeal of Decision Under Sections 245A or 210 of the Immigration and Nationality Act	I-694	1615-0034
Application to Adjust Status from Temporary to Permanent Resident (Under Section 245A of Public Law 99-603)	I-698	1615-0035
Refugee/Asylee Relative Petition	I-730	1615-0037
Application for Employment Authorization	I-765	1615-0040
Application for Family Unity Benefits	I-817	1615-0005
Application for Temporary Protected Status	I-821	1615-0043
Application for Action on an Approved Application or Petition	I-824	1615-0044
Sponsor's Notice of Change of Address	I-865	1615-0076
Application for T Nonimmigrant Status	I-914	1615-0099
Application to File Declaration of Intention	N-300	1615-0078
Application to Preserve Residence for Naturalization Purposes	N-470	1615-0056
Application for Replacement Naturalization/Citizenship Document	N-565	1615-0091
Application for Certificate of Citizenship	N-600	1615-0057
Application for Posthumous Citizenship	N-644	1615-0059
Application for Replacement of Form I-688a or I-688	I695	1615-0000
Premium Processing	I-765PP	1615-00040
Application for Vol Departure Under Family Unity Program	I-817	1615-0005