Privacy Impact Assessment
for the

Computer Linked Application Information Management System (CLAIMS 4)

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 W. Kropf
Acting Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

This Privacy Impact Assessment (PIA) analyzes the Computer Linked Application Information Management System (CLAIMS) 4. CLAIMS 4 is the Department of Homeland Security (DHS) United States Citizenship and Immigration Service's (USCIS) system for processing Applications for Naturalization. USCIS is conducting this PIA to document, analyze, and assess its current practices with respect to the personally identifiable information it collects, uses, and shares; and to improve its ability to provide appropriate citizenship and immigration status information to users.

Overview

USCIS is responsible for the administration of immigration and naturalization adjudication functions, and for establishing immigration services, policies, and priorities. In executing its mission, USCIS performs functions that include adjudications of:

(1) immigrant visa petitions;

(2) asylum and refugee applications; and

(3) naturalization applications.

CLAIMS 4 is an electronic case management application tracking and processing system. USCIS uses the system as automated support for the variety of tasks associated with processing and adjudicating N-400 Applications for Naturalization. Naturalization is the process by which a foreign citizen or national acquires U.S. citizenship after he or she fulfills the requirements established by Congress in the Immigration and Nationality Act (INA). The general requirements for completing the administrative naturalization process include:

- Period of continuous residence and physical presence in the United States
- Three months residence in a particular USCIS district prior to filing
- Ability to read, write, and speak English (applicant will be asked to read out loud and write sentences in English during their interview)
- Knowledge and understanding of U.S. history and government
- Good moral character (e.g., no criminal convictions or other disqualifying conduct as stated in the Immigration and Naturalization Act)
- Attachment to the principles of the U.S. Constitution
- Favorable disposition toward the United States.

CLAIMS 4 functions include the receipting, data entry, and other initial operations necessary to process naturalization applications (e.g. background checks). In addition to these functions, CLAIMS 4 information is also used in support of adjudications and naturalization oath ceremony management activities conducted at local USCIS offices.

USCIS personnel responsible for adjudicating and supervising naturalization cases and USCIS clerks supporting these functions use CLAIMS 4 at USCIS headquarters, service centers, local offices, and Application Support Centers (ASC) to track the naturalization adjudication process from application to granting or denying of the benefit.

CLAIMS 4 contains the following types of personally identifiable information (PII): names and addresses, telephone numbers, birth information, death information, Social Security Numbers (SSN), country of citizenship, applicant and family members' immigration status, marital and family status data, information regarding personal characteristics, information regarding tax and financial, employment information, medical information, military and selective service information, information regarding organization membership or affiliation, and criminal history information (to the extent such history is revealed by the applicant in their application) CLAIMS 4 also indicates some of the background checks (name and fingerprint based) that an applicant has completed and whether a response is available.

Naturalization Process.

In order to begin the naturalization process, an individual must complete form N-400. [1] Upon completion, the applicant submits the application to the service center for his or her region. The applicant must submit the following with the completed N-400: two color photographs, a copy of his or her Permanent Resident Card (aka "Green Card"), and a check or money order to pay the application fee and biometric fee (a fee to pay for fingerprinting). Applicants must also submit additional documentation with their applications under certain circumstances. [2]

USCIS employees at all service centers receive completed N-400 forms and supplemental documentation from the applicants via regular mail. Once the application is received, USCIS personnel manually enter the applicant's information from the form into the CLAIMS 4 server at the service center. When certain data elements from the N-400 are entered into CLAIMS 4, the system automatically generates an application identification number, which may be used later to check the status of the application. After USCIS personnel enter information from the application into the system, USCIS sends an appointment letter to the applicant indicating when and where the applicant must go to have his of her fingerprints taken.

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) in order to conduct background checks. If an applicant is overseas or is 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.

After the fingerprints are taken, the applicant must wait for USCIS to schedule a personal interview. 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 background checks are conducted. Biographic and biometric data collected in order to conduct background checks are sent 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.

Prior to the personal interview, USCIS conducts background checks on the applicant to ensure all eligibility requirements are met. In order to facilitate these background checks, CLAIMS 4 shares the PII with the FBI and DHS Customs and Border Protection (CBP) to conduct name-based and fingerprint-based criminal history background checks.

In addition, CLAIMS 4 shares the following information with other USCIS systems to process the application and verify the accuracy of information provided by the applicant. Central Index System (CIS);

---

[1] *See,* USCIS Publication, *A Guide to Naturalization*, Form N-476, http://www.uscis.gov

[2] *See, A Guide to Naturalization*, at p. 47 (Document Checklist) for a list of documents that must be submitted in certain circumstances.

Verification Information System; Reengineered Naturalization Automated Casework System (RNACS); CLAIMS 3 Mainframe; Biometric Benefits Support System (BBSS) Refugee, Asylum and Parole System (RAPS); Receipt and Alien-File (A-File) Accountability and Control System (RAFACS); Performance Analysis System (PAS); National File Tracking System (NFTS), Complete File Review, Change of Address, and Customer Relations Information System.

Upon successful completion of the background checks, USCIS will schedule a personal interview. N-400 applications require a personal interview, which assists USCIS examiners in evaluating the applicant's status and eligibility for naturalization. Before the interview, the applications are forwarded from the service center to the field office where USCIS will conduct the interview. At the completion of the application and interview process, the applicant's Application for Naturalization is either granted, denied or withdrawn (e.g., withdrawal may occur, for example, if the applicant has multiple pending applications).

Throughout this process, CLAIMS 4 data may be shared within DHS for fraud detection or national security purposes.

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

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 4 contains data entered from the N-400, *Application for Naturalization,* as well as data generated by DHS or the FBI. Additional information is sometimes obtained verbally from applicants during interviews. The following data elements are entered into the system from the N-400 application:

Applicant Provided Information

Names: USCIS collects names (first, middle or initial, family, aliases, maiden, current/prior spouse's, children's, person who prepared the form) in CLAIMS 4 to identify the applicant and verify the accuracy of information provided in an application.

Addresses: USCIS collects addresses (home, current and prior spouse's, children's, applicant's e-mail, person who prepared the form, applicant's/spouse's employer) in CLAIMS 4. USCIS uses the addresses to send information to and obtain information from the applicant (e.g., denial or grant of an application, and/or requests for additional information) to establish eligibility for naturalization.

Telephone Numbers: USCIS collects telephone numbers (e.g. applicant's telephone number, form preparer's telephone number) in CLAIMS 4 to be used in the event that USCIS needs to contact the applicant or the form preparer with questions regarding information contained in the completed forms.

Birth Information: USCIS collects birth dates (applicant, spouse, and children), and country of birth in CLAIMS 4 to verify the identity of the applicant and to determine his/her eligibility for naturalization.

Social Security Numbers: USCIS collects SSNs (applicant and current spouse) in CLAIMS 4 to

verify the identity of the applicant and spouse and to determine their eligibility for certain benefits.

Citizenship/Nationality Information: USCIS collects citizenship information (applicant's race/country of nationality, spouse, date current spouse obtained citizenship, place spouse became a citizen) in CLAIMS 4 to determine an applicant's eligibility for naturalization, for statistical purposes, to conduct background investigations and to detect possible fraud in the application process (e.g., comparing the race stated in the application with the race of the person appearing for the naturalization interview).

Information Regarding Immigration Status: USCIS collects information from the applicant regarding immigration (applicant, current/prior spouse's A-Number) and dates the applicant entered into and exited from the U.S. (days spent outside the U.S., trips outside the U.S.) in CLAIMS 4 to determine their eligibility for naturalization.

Marital Status/Family Information: USCIS collects marital information (e.g., current and prior marriages or prior separations, prior spouses, date of marriage/divorce, number of marriages for applicant and spouse, reason prior marriage ended, whether applicant has ever been married to multiple persons at the same time) and family information (number of children) in CLAIMS 4 to verify the validity of the information provided in an application and to determine the applicant's eligibility for naturalization (e.g., to determine whether s/he is a bigamist).

Personal Characteristics: USCIS collects information regarding personal characteristics (hair color, eye color, height, gender, weight, languages spoken) in CLAIMS 4 for identification purposes and to reduce the risk of fraud (e.g., receipt of benefits using someone else's information).

Tax Payment and Financial Information: USCIS collects tax payment information (failed to pay taxes, owes taxes, claimed non resident status for tax purposes, failed to file taxes because of nonresident status) and financial information (applicant/spouse's earnings per week; amount in bank accounts; value of vehicles, real estate, and others assets; parents' estimated assets/weekly earnings) in CLAIMS 4 to determine whether the applicant is capable of supporting themselves financially, whether they are likely to follow the law if naturalized, to ensure compliance with statutory and regulatory requirements and determine eligibility for naturalization.

Employment Information: USCIS collects employment information (place and address of employment/occupation, type of work, employer name, length of employment, spouse's employment) in CLAIMS 4 and to determine the applicant's eligibility for naturalization.

Medical Information: USCIS collects medical information (disability requiring accommodation, alcoholism, declaration of incompetence, family medical history) in CLAIMS 4 to determine whether the applicant requires an accommodation (e.g., during interviews), poses a medical threat to others or a potential financial burden to the U.S. if naturalized.

Military and Selective Service Information: USCIS collects information evidencing Selective Service registration and military service (e.g., Selective Service number, date of registration, application for military exemption, military branch, willingness to bear arms for the U.S.) in CLAIMS 4 to verify that the applicant has registered with Selective Service as required by law and to ensure eligibility for naturalization.

Information Regarding Organization Membership or Affiliation. USCIS collects information regarding an applicant's organization memberships and affiliations (organizations, associations, clubs, foundations, parties, societies, or similar groups; communist party membership; totalitarian party membership; terrorist organization membership) in CLAIMS 4 to determine whether the applicant poses a security threat to the U.S. or individuals if naturalized.

Criminal History or Involvement and Moral Character Issues. USCIS collects information regarding an applicant's criminal history, involvement in criminal activities and information regarding moral character in CLAIMS 3 to assess whether the applicant meets the statutory requirements needed to

become naturalized. USCIS is required by statute (6 U.S.C. 1424) to collect certain information to assess an applicant's fitness for naturalization. USCIS uses this information to determine whether the applicant has ever:

- been a habitual drunkard;
- sold or smuggled controlled substances, illegal drugs, or narcotics;
- advocated the overthrow of any government by force or violence;
- committed a crime or offense but was not arrested;
- been arrested, received a citation, been detained by law enforcement;
- been charged with committing a crime or offense; been convicted of a criminal act or offense;
- been placed in rehabilitative sentencing or rehabilitative program (e.g., diversion program);
- received a suspended sentence or been placed on probation or parole; s
- pent time in jail or prison;
- been a prostitute or procured anyone for prostitution;
- helped anyone enter the U.S. illegally;
- been married to more than one person at the same time;
- engaged in illegal gambling or received income from illegal gambling;
- failed to pay alimony or support dependents; sought immunity from prosecution (i.e., to determine fitness for naturalization);
- given false or misleading information to U.S. government officials while seeking naturalization or to prevent deportation, exclusion or removal;
- lied to U.S. officials to gain entry into the U.S.;
- been deported, removed, or excluded from the U.S. or current participation in such proceedings;
- been or filed for relief from being excluded removed, or deported from the U.S.;
- been affiliated with the Communist Party or any other totalitarian party or terrorist organization;
- participated in genocide or persecution because of race, religion, national origin, or political opinion;
- from 1933 through 1945 worked or associated directly or indirectly with the Nazi government of Germany, any government occupied allied with or established with the help of the Nazi government of Germany, or any German Nazi or SS unit, paramilitary unit, self-defense unit, vigilante unit, citizen unit, police unit, government agency or office, extermination camp, concentration camp, prisoner of war camp, prison labor camp or transit camp;
- left the U.S. to avoid a military draft; or
- deserted U.S. Armed Forces.

DHS and FBI generated information

CLAIMS 4 generates certain information and maintains the status of certain activities related to the adjudication process.

USCIS Generated Information

CLAIMS 4 generates an application identification number that allows an applicant to check the status of the benefit, and scheduling information related to interviews, oath ceremonies, and fingerprinting.

Background Check Information Stored in CLAIMS 4

USCIS conducts three different background checks on persons applying for Naturalization: (1) A Federal Bureau of Investigation (FBI) fingerprint check, (2) a FBI name check, and (3) a DHS Customs and Border Protection (CBP) Treasury Enforcement Communication System/Interagency Border Inspection System (TECS/IBIS) name check.

The only results from the FBI background checks that are stored in CLAIMS 4 are:

- basic information regarding the FBI name check (i.e., "Pending" [because the search is ongoing], "No Record" or a "Positive Response"), or
- fingerprint check results (Unclassifiable [i.e., prints rejected because of image quality], Non-Identification ["Non-Ident" meaning no records on file], or Identification ["Ident" meaning records are on file]) and the date of the response.

The basic FBI name check results are also stored in the USCIS 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 4 or the FBI Query System. The actual substantive information discovered during FBI background checks is sent by the FBI to USCIS in paper form and is not uploaded to any USCIS system. USCIS adjudicators access the applicant's paper file, i.e. the A-File, to get information necessary to process applications

Information relating to the FBI Name Check is stored in the USCIS system, FBI Query. If the FBI Query System indicates that there is a positive response from the FBI and the report is not in the A file, the adjudicator can contact the National Benefits Center (NBC) to see if they have received the report and find out what the disposition is. (All FBI reports from the FBI Name Check process are sent to the NBC for tracking and dissemination.) If it is determined that a new report has to be ordered, the adjudicator can send a new name check request to USCIS HQ where that request will be consolidated with other FBI name check requests and sent to the FBI.

Information relating to the FBI Fingerprint Check is stored in USCIS's system, BBSS. If the RAP sheet from the FBI fingerprint check is not in the A file, the adjudicator can go to BBSS and view the RAP sheet.

If for some reason the results of an FBI background check are not in the A-File when examined by a USCIS adjudicator, the adjudicator would verify the background check results in CLAIMS 4. If the name check result in the FBI Query System is "Pending", the adjudicator would check with the FBI to determine the status of the search. If the name check was "Positive" the adjudicator would look in BBSS to verify the actual information (e.g., RAP sheets or other criminal history information) discovered during the name check.

The adjudicator would contact the FBI to obtain the actual information (e.g., RAP sheets or other criminal history information), if any, discovered during the FBI fingerprint check if the fingerprint check result in CLAIMS 4 is "Ident" or "unclassifiable" (for a fingerprint check").

The TECS/IBIS query results are not stored in CLAIMS 4. If the TECS/IBIS search indicates there may be a match, no substantive information is sent to CLAIMS 4. Instead the user logs directly into TECS/IBIS to find the detailed information. The detailed information related to any TECS/IBIS results are printed, marked "For Official Use Only," and stored in the applicant's paper A-file. If for some reason the results are not found in the applicant's A-File, the adjudicator would access TECS/IBIS directly to obtain the information.

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 information technology systems, BBSS and ISRS, are being phased out and will soon be replaced by the Biometric Storage System (BSS).[3] Both are coved by the BSS System of Records Notice (SORN). Similarly, the information technology systems, USCIS FBI Query, FD-258 EE, and FD-258 Mainframe will soon be replaced by the Background Check System (BCS).[4] Again these are covered by the BCS SORN.

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

The source of most of the information in the system is the completed N-400, *Application for Naturalization*, which is submitted by applicants seeking benefits and validated by applicants when interviewed.

CLAIMS 4 also obtains information from the following internal USCIS systems:

USCIS, Central Index System. CIS supports USCIS records management by collecting, storing, and disseminating PII about individuals of interest to the agency (e.g., persons who file applications and their family members). CIS currently provides information to organizations granting benefits and recording subsequent status changes; documents chain of custody for enforcement (i.e., all documents submitted during the naturalization process and when they were submitted); provides 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; 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), who were investigated by the DHS in the past, or who are suspected of violating immigration-related laws or regulations. When an application is entered into CLAIMS 4, verification data is sent to CIS that consists of an applicant's A-Number, name, date of birth, and country of birth. CIS then sends verification results back to CLAIMS 4. The verification results are then used to validate that the information provided by the applicant matches the information in CIS. At the end of the CLAIMS 4 process, after an applicant has been naturalized, the naturalization information (i.e., name, date of birth, country of birth, date naturalization certificate was issued, certificate number and court code) is sent to CIS.

---

[3] See BSS PIA at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_bss.pdf

[4] See BCS PIA at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_bcs.pdf

USCIS, Receipt and Alien-File Accountability and Control System. RAFACS is the file management system in use at three of the USCIS service centers. The CLAIMS 4 interface with RAFACS allows insertion of the case number of an N-400 application receipt file and checks to determine if a particular A-File is present at a processing site. If not, the files are retrieved through CIS transfer requests until the files arrive on site, or when a diligent search process has been satisfied. A diligent search is conducted in an attempt to find the file. If it still cannot be found in the system after three searches, a temporary file is created. CLAIMS 4 users at service centers are able to query RAFACS for the location of A-Files on site at any stage of naturalization processing. This interface updates CLAIMS 4 to reflect the status of A-Files requested from other sites, so that cases waiting for those files can be released for the scheduling of interviews.

USCIS, Refugees, Asylum and Parole System. RAPS provides automated support to USCIS in the implementation of the Refugee Act of 1980. This Act created a statutory basis for asylum in the United States and made withholding of deportation for those who qualify for asylum mandatory rather than discretionary. The information derived from Applications for Asylum is entered into RAPS and an output file is created containing the application data (e.g., date received, office code, applicable service center etc.), applicant data (e.g., biographic information, address, attorney's name, A-Number, SSN) and a fingerprint scheduling request. This output file is then transferred to CLAIMS 4.

USCIS, Performance Analysis System. To provide immigration benefit services in a timely manner, USCIS uses PAS on a monthly basis to collect performance data on applications received, completed, and pending. The PAS application is a centralized, online, integrated data management system that automates the tracking of field operations data. This field operations data includes workload accomplishments and resource expenditures for a wide range of USCIS activities, including examinations, enforcement, and management. PAS allows USCIS users (including CLAIMS 4) from regional, district, and field offices to enter, access, and report information that pertains to their office or program area. CLAIMS 4 sends PAS claim counts (numbers regarding complaints filed), and PAS sends CLAIMS 4 statistical results.

USCIS, Reengineered Naturalization Automated Casework System. RNACS is the predecessor system of CLAIMS 4. It contains some of the same information contained in CLAIMS 4 (e.g. applicant name, address, date of birth, country of birth/citizenship, sex, marital status, height, SSN, fingerprints).. RNACS processes application information related to naturalization applications that predated CLAIMS 4. Once per day (Monday through Friday), CLAIMS 4 transmits N-400 data (applicant name, address, date of birth, country of birth/citizenship, sex, marital status, height, SSN, fingerprints) to RNACS electronically over the USCIS Mainframe. A confirmation record is written for each file record and returned back to CLAIMS 4 for validation of RNACS processing.

USCIS Index Cards. CLAIMS 4 also collects information from paper index cards containing basic demographic data on individuals with respect to cases that were adjudicated before the CLAIMS 3, CLAIMS 4, and USCIS CIS were established.

CLAIMS 4 also collects information from the following external source:

Federal Bureau of Investigation Fingerprint Check and Name Check. As discussed in Section 1.1, CLAIMS 4 receives personal information from the FBI after the completion of an FBI Name Check and an FBI Fingerprint Check. The only results from any of the four background checks that are stored in CLAIMS 4 is the basic information regarding the FBI name check (i.e., "Pending" [because the search is ongoing], "No Record" or a "Positive Response") or fingerprint check results (Unclassifiable [i.e., prints rejected because of image quality], Non-Identification ["Non-Ident"], or Identification ["Ident"]) and the date of the response. The actual information (e.g., RAP sheets or other criminal history information) discovered during the FBI background checks is not stored in CLAIMS 4. The actual substantive information discovered during FBI background checks is sent by the FBI to USCIS in paper form and is not uploaded to any USCIS system. USCIS adjudicators access the applicant's paper file to get information necessary to process

applications. The sharing of information between USCIS and the FBI is conducted pursuant to an agreement between INS and the FBI that predated the creation of DHS. An updated agreement between DHS USCIS (formerly INS) and the FBI is currently being negotiated.

CLAIMS 4 does not contain information obtained from public websites, data brokers, commercial aggregators and/or other private entities. Information is obtained from sources other than the individual because part of the process supported by CLAIMS 4 requires the verification of information received from the applicant. CLAIMS 4 also contains reports or information regarding adjudications and determinations made by USCIS employees with respect to applications. The system itself does not create a score, analysis, or report, but it does contain conclusions reached by USCIS personnel regarding applicants' eligibility for naturalization based on human analysis of applications and supporting data.

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

All information collected from applicants or maintained by CLAIMS 4 is required to establish the applicant's identity, history with USCIS, and eligibility for naturalization. This information is entered into CLAIMS 4 to assist the adjudicator in making a decision regarding the application, and to help ensure equitable treatment of applicants, compliance with legislative mandates, and proper implementation of agency policies and regulations.

Title 8 U.S.C. Section 1324a requires background checks for all applicants. Background checks are conducted to determine whether the applicant has any criminal history that might affect his or her application. To conduct background checks with respect to naturalization applications, USCIS requires the collection of biometrics (fingerprints). Name, date of birth, and fingerprints are used to perform background checks. Photographs and signatures are also collected to issue a certificate signifying receipt of a benefit. Signatures are also collected to memorialize the applicant's promise that the information in the application is correct. Applications without signatures are not accepted.

Please see Section 1.1 for a discussion of the reason that each data element is collected.

CLAIMS 4 does not collect, use, disseminate, or maintain commercial data.

1.4 How is the information collected?

Most of the information in CLAIMS 4 comes from the completed USCIS form N-400, *Application for Naturalization* (OMB Control Number 1615-0052). This form is submitted by the applicant (or his or her representative) by mail and USCIS employees and contractor staff enter the information into CLAIMS 4. Electronic filing is not available for the N-400. Completed application forms must be sent to the appropriate service center for processing. Applicants may also file a petition for a name change in order to update their information in the system.

Photographs are submitted by the applicant with the N-400. Fingerprints are also required in order to complete the application process. This process begins when the applicant provides the requested information on a fingerprint card (form FD-258) or appears at the appropriate Application Support Center (ASC) for biometric capturing. Applicants do not, however, submit their fingerprints to USCIS with their applications. USCIS contacts applicants by mail to inform them of the time and place where their fingerprints will be taken at specified ASC locations.

Information in CLAIMS 4 may also originate from notes taken by USCIS personnel during interviews with the applicant. This field in the CLAIMS 4 system is rarely used and data input is very narrow in scope on the rare occasion when it is populated.

See section 1.2 for a discussion of the manner in which and purpose for which CLAIMS 4 collects information from internal and external sources.

1.5 How will the information be checked for accuracy?

When N-400 applications and other forms are received by the service centers, they are placed in receipt files and the applicant's A-File. Standard Operating Procedures (SOPs) include detailed quality control reviews that help ensure that the data has been accurately entered into CLAIMS 4 from naturalization applications. These SOPs include strict procedures for handling applications and for data transfer from paper forms to CLAIMS 4. They ensure that all data fields are completed and describe how data entry personnel must handle inconsistencies and discrepancies in data entries. The SOPs cover every stage of data entry from the time the envelope is opened until the time the data is entered into CLAIMS 4 and the file is ready to be sent to the appropriate field office that will conduct the interview.

If upon later review an applicant determines that information in the system is incorrect, 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. In addition, the accuracy of the data entry can be challenged during the interview process.

CLAIMS 4 information is also checked for accuracy through database technical controls (e.g., a program that checks the zip code to ensure it matches the city, state and street), inherent business logic built into the system, and a manual review process (e.g., interviews with the applicants).

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 4 comes from 8 U.S.C. Section 1101 *et seq*. 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 Director pursuant to a departmental management directive. In addition, the Office of Management and Budget (OMB) has approved the content and format of the N-400, *Application for Naturalization*.

CLAIMS 4 contains information that may indicate a person's religious or other organizational affiliation. This information is maintained in CLAIMS 4 when:

1. It is reported on the N-400 to determine affiliations that may affect eligibility for naturalization, derived from the following subsections of 8 U.S.C. 1182, Subchapter III, *Nationality And Naturalization*:

   - §1424. *Prohibition Upon The Naturalization Of Persons Opposed To Government Or Law, Or Who Favor Totalitarian Forms Of Government*
   - § 1428. *Temporary Absence Of Persons Performing Religious Duties*
   - § 1182. *Inadmissible Aliens* (b)(III)(D) *Immigrant Membership In A Totalitarian Party*

2. 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 entering information into CLAIMS 4 from forms submitted by applicants.

Mitigation: USCIS has mitigated this potential risk by developing detailed SOPs for handling information collected in the N400 Application for Naturalization. These SOPs include detailed quality control reviews that help to ensure that the information has been accurately transferred from the N400 submitted by applicants into CLAIMS 4. 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 4 and saved. USCIS also mitigates this risk by allowing applicants Privacy Act access to their data so they can get access to and request changes 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. Corrections can also be made during the interview process.

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 (which includes PII). Additionally, all DHS employees are required to take annual computer security training, which includes training on appropriate use of sensitive data and proper security measures. Employees are required to follow Rules of Behavior contained in the DHS Sensitive Systems Handbook.

USCIS also employs SOPs at the service centers to ensure accurate data entry and proper handling and appropriate use of information. In addition, audit trails are used to track all CLAIMS 4 user transactions

(e.g., data entry, file requests, fees received, etc.). Disciplinary rules are in place to ensure appropriate use of CLAIMS 4 information.

Privacy Risk: Additional privacy risk that was identified was the non systematic printing of TECS/IBIS results and saving them in the paper A-File.

Mitigation: The Standard Operating Procedures have been updated to ensure that if there are TECS/IBIS results for an applicant, the information is printed, marked FOUO, and placed in the paper A-File.

Privacy Risk: Additional privacy risk is that inaccurate information will be used to deny a benefit.

Mitigation: The risk of inaccurate information being used to deny a benefit is reduced by the fact that information is (1) collected in large directly from the individual on the application, (2) technology has been deployed to find common key errors, and (3) 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.

Section 2.0 Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

All data in CLAIMS 4 is used to adjudicate applications for naturalization and to identify possible immigration fraud or national security interests.

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 or TECS/IBIS 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 4 could be provided to law enforcement agencies in the interest of public safety.

The CLAIMS 4 application is divided into modules, or subsystems, which support CLAIMS 4's major functions. A module is a collection of functions that work together to satisfy a major CLAIMS 4 business process. CLAIMS 4 architecture is made up of the following major modules:

(1) ***Mailroom Entry.*** Allows users at the service centers to input the information (time and date received) from applications, assign each application a system-generated application identification number, and print the application identification number (AppID) on a bar code label. This module is also used to endorse, and assign payment ID numbers to payments that accompany applications submitted.

(2) ***Data Entry.*** Allows the user to enter application information (e.g., from the N-400 or I-881 [*Application for Suspension of Deportation or Special Rule Cancellation of Removal*]) into CLAIMS 4.

(3) ***Finance.*** Used by contractor personnel to process payments and perform accounting functions in CLAIMS 4.

(4) ***Adjudication.*** Used to assist district adjudication officers in the interview process. Application information can be reviewed and updates made to this module. Adjudication decisions can also be recorded.

(5) ***Case Status.*** Enables USCIS personnel to view case information. This module displays all case histories as well as the current status of the case.

(6) ***Case Management (CM).*** Used to resolve data discrepancies between CLAIMS 4 and the Central Index System, and to update case and address information.

(7) ***Scheduler/Batch Scheduler.*** Used to schedule applicants for interviews, oath ceremonies, and fingerprinting. It is also used to view information related to scheduling.

(8) ***Notice.*** Used to print or reprint notices created to inform applicants and their representatives (where applicable) of scheduled appointments and the status of their applications. The notices are sent by mail after being generated by the system.

(9) ***Reporting.*** Used to generate and print reports related to CLAIMS 4. Reports can be requested according to functional areas available to the current user. Each area contains several types of reports, each with unique query criteria selection fields (e.g., name, Alien Registration Number [A-Number], date of birth, country of citizenship, and AppID).

(10) ***Oath Ceremony Management.*** Used to print, view, and share naturalization certificate information within USCIS .

(11) ***System Maintenance.*** Enables systems administrators to assign individual user privileges and determine local maintenance settings.

(12) ***Workflow Administration.*** Enables a system administrator to monitor and reset activities for a case.

(13) ***Military Case Module***. Enables the processing of applications filed by members of the military. This separate module exists to address the unique issues (and evidentiary requirements) that arise from naturalization requests from members of the military who are overseas.

Background Checks

USCIS conducts three different background checks on persons applying for Naturalization: (1) A Federal Bureau of Investigation (FBI) fingerprint check, (2) a FBI name check, and (3) a DHS Customs and Border Protection (CBP) Treasury Enforcement Communication System/Interagency Border Inspection System (TECS/IBIS) name check.

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 to be used for any authorized general law enforcement or background check purpose to which the information might be relevant.

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

Attache 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 (the FBI information sheet [informally known as a Records of Arrests and Prosecutions (RAP) sheet] or a no match response) are stored in USCIS' FBI Query system. The RAP sheet contains the date of and reason for an arrest.

The results of the FBI Name Check are stored in CLAIMS 4. This includes the response from the FBI (whether or not the FBI has a record for that applicant, not the substantive information [e.g., RAP sheet information] found), whether it be a pending (interim) response or a final response, and the USCIS terminology used to interpret the FBI response (i.e., positive identification ("IDENT") or No Record).

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 4 applicants are extracted from, CLAIMS 4, formatted for TECS/IBIS processing, and transferred electronically to the Vermont Service Center via FTP server. The Vermont Service Center then uploads the information to TECS/IBIS.

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 sent back to USCIS (via the process above in reverse order). If the TECS/IBIS search indicates there may be a match (i.e., a "HIT"), no substantive information is sent to CLAIMS 4. Instead, the user logs directly into TECS/IBIS to get the detailed information. This substantive 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.

USCIS Use of Background Check Results Information

Background check result information encompasses data received from the FBI as well as DHS (TECS/IBIS) systems. 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), and information from the TECS/IBIS database.

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

USCIS does not use CLAIMS 4 to perform complex analytical tasks resulting in data matching such as relational analysis, scoring, reporting, or pattern analysis. The system itself does not make available new or previously unavailable data from newly derived information. USCIS human analysts do, however, collect data from applications 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). The outcome

of this analysis 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 as described in this document.

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 4.

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.

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. Additionally, all DHS employees are required to take annual computer security training, which includes training on appropriate use of sensitive data and proper security measures. Employees are required to follow Rules of Behavior contained in the DHS Sensitive Systems Handbook.

USCIS also employs SOPs at the service centers to ensure accurate data entry and proper handling and appropriate use of information. In addition, audit trails are used to track all CLAIMS 4 user transactions (e.g., data entry, file requests, fees received, etc.). Disciplinary rules are in place to ensure appropriate use of CLAIMS 4 information. Only users who have a need to know PII are allowed access.

Risk: Individuals who have legitimate access to PII could exceed their authority to expedite or inappropriately grant or deny the benefit.

Mitigation: USCIS has split adjudication responsibilities so that more than one individual must approve for naturalization benefits to be granted or denied. Additionally, USCIS's internal affairs conducts audits to ensure that the standard operating procedures are followed.

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?

Electronic data in the CLAIMS 4 repository will be deleted 15 years after the application for naturalization is granted, denied, or withdrawn and any appeals process (if applicable) is completed. Information 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. All CLAIMS 4 information is maintained in accordance with the criteria approved by the National Archives and Records Administration (NARA).

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

NARA approved the retention schedule for CLAIMS 4 on June 25, 2003.

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: Maintaining personal information for a period longer than necessary to achieve agency objectives.

Mitigation: Although there is always risk inherent in retaining personal data for any length of time, the CLAIMS 4 data retention periods identified in the NARA schedule are consistent with the concept of retaining personal data only for as long as necessary to support the agency's mission. The schedule proposed and approved by NARA matches the requirements of the Federal Records Act and the stated purpose and mission of the system. The time periods in the NARA schedule 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 purposes?

CLAIMS 4 shares data internally with:

DHS CBP TECS/IBIS: The names and dates of birth of applicants for Naturalization are extracted from CLAIMS 4, formatted for TECS/IBIS processing, and transferred electronically to the Vermont Service Center via FTP server. The Vermont Service Center then uploads the information to TECS/IBIS. TECS IBIS then runs a background check in order to determine whether the applicant is eligible for the benefit sought. See Section 2.1 (under heading "TECS/IBIS Name Check") for a detailed discussion of the data shared with CBP TECS/IBIS.

DHS Verification Information System. CLAIMS 4 provides VIS with verification of naturalization status through the Person Centric Query (PCQ) service. The PCQ Service is a multi-system query tool that allows USCIS to more efficiently and effectively check USCIS databases to determine identity and immigration status (including employment eligibility). The purpose of this multi-system check is to identify possible identity fraud.

USCIS, Office of Fraud Detection and National Security (FDNS). FDNS is given read only access to CLAIMS 4 on a case-by-case basis in order to identify potentially fraudulent applications for immigration benefits. FDNS officers use their read only access to conduct manual searches of the CLAIMS 4 database to determine whether there are inconsistencies in the information contained within CLAIMS 4 that might indicate fraud. If a FDNS Officer identifies suspicious activities that indicate a potentially fraudulent application for immigration benefits, either from a tip or by searching the CLAIMS 4 database, a lead is

opened in the Fraud Detection and National Security Data System (FDNS-DS) and a FDNS-DS identifier is automatically generated. FDNS developed the FDNS-DS to identify and decrease fraud in the immigration process. Once a FDNS Officer initiates an inquiry from inconsistencies found in CLAIMS 4, they may pull data from CLAIMS 4, including: Subject Name(s); Subject Social Security Number (SSN); Subject Date of Birth (DOB); Subject Country of Birth (COB); Subject Maiden Name; Subject Address; Taxpayer ID; Telephone Number; Alias Name(s); and Alien Registration Number (A-Number).

Image Storage and Retrieval System (ISRS). Biometrics and biographic data collected to conduct background checks are stored in 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.

DHS ICE and CBP Investigators. DHS ICE and CBP investigators access CLAIMS 4 to verify information given to them by aliens and others during the course of investigations (e.g., if an agent is told someone was naturalized, a verification check may be conducted).

DHS Intelligence and Analysis (I&A). DHS I&A analysts may access CLAIMS 4 information for national security purposes.

USCIS, Performance Analysis System. PAS allows USCIS users (including CLAIMS 4) from regional, district, and field offices to enter, access, and report G-23 (PAS form that documents performance workload measures) information (non-PII) that pertains to their office or program area. CLAIMS 4 sends PAS claim counts (numbers of complaints filed), and PAS sends CLAIMS 4 statistical results. For a full discussion of PAS, please see Section 1.2.

USCIS, Central Index System. CIS supports USCIS records management by collecting, storing, and disseminating PII related to individuals of interest to the agency. When an application is entered into CLAIMS 4, verification data is sent to CIS that consists of an applicant's A-Number. CIS then sends verification results (the applicant's A-Number) back to CLAIMS 4. At the end of the CLAIMS 4 process, after an applicant has been naturalized, the naturalization information (name, date of birth, country of birth, date naturalization certificate was issued, certificate number and court code) is sent to CIS. For a full discussion of CIS, please see Section 1.2.

USCIS, CLAIMS 3. CLAIMS 4 receives information from and sends information to CLAIMS 3 regarding *Change of Address* forms (Form AR-11) to ensure that both systems are current and accurate. CLAIMS 4 also interfaces with CLAIMS 3 for the purpose of scheduling interviews to adjudicate I-485, *Applications to Register Permanent Residence or Adjust Status*.

Customer Relationship Interface System (CRIS). CRIS enhances USCIS's ability to provide consistent, timely, and accurate status information to customers and their representatives. CRIS provides USCIS customers access to CLAIMS 4 case status information through a web-based application on the Internet, and via an Interactive Voice Response system on a toll-free telephone line. It also allows call handlers and field staff to efficiently collect and/or report the status of Change of Address, Case Status, and Appointment Scheduling Referrals. The system provides USCIS field operations and managers with the ability to collect, process, and manage Change of Address, Case Status, and Appointment Scheduling Referrals through an intranet application supported by a shared database. CRIS does not interface directly with the CLAIMS 4 system. Custom software is used to push CLAIMS 4 case status data out to the CRIS database automatically at a scheduled, predetermined time each day.

Reengineered Naturalization Automated Casework System (RNACS). RNACS is the central repository of information on naturalization applications. Once per day (Monday through Friday), CLAIMS 4 transmits N-400 data (applicant name, address, date of birth, A-Number, country of birth/citizenship, sex, marital status, height, SSN, fingerprints) to RNACS electronically over the USCIS Mainframe. For a full discussion of RNACS, please see Section 1.2.

4.2 How is the information transmitted or disclosed?

Except as otherwise stated in Section 4.1, all internal sharing is conducted over a secure and reliable DHS electronic interface or secure courier. This interface utilizes secure network connections on the DHS core network. 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.

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 CLAIMS 4 PII (including searches beyond the scope of the user's duties) both during transmission and after it is shared.

Mitigation: User access to CLAIMS 4 data is limited to those who need the information to perform their job functions. All authorized users must authenticate using a user ID and password. DHS policies and procedures are in place to limit the use of and access to all data in CLAIMS 4 to the purposes for which it was collected. Computer security concerns are minimized by the fact that the information shared internally remains within the DHS environment. An audit trail is kept for system access and all transactions that request, create, update, or delete information from the system. The audit trail/log, which includes the date, time, and user for each transaction, is secured from unauthorized modification, access, or destruction.

All DHS employees and contractors are required to follow DHS Management Directive (MD) Number: 11042, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, May 11, 2004. This guidance controls the manner in which DHS employees and contractors must handle Sensitive but Unclassified/For Official Use Only Information. All employees and contractors are required to follow Rules of Behavior contained in the DHS Sensitive Systems Handbook. Additionally, all DHS employees are required to take annual computer security training, which includes training on appropriate use of sensitive data and proper security measures.

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?

Federal Bureau of Investigation Fingerprint and Name Check Systems. As mentioned in section 1.1 of this PIA, all naturalization applicants are required to have several criminal background checks completed. 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 order to conduct criminal background checks. This information is sent to the FBI for fingerprint and name

check background searches as stated in more detail above.

Information may also be shared in compliance with the published Privacy Act System of Records Notice, such as the intelligence community, state and local law enforcement.

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 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 to be used for any authorized general law enforcement or background check purpose to which the information might be relevant

All external sharing is covered by an appropriate routine use as stated in System of Records Notice (SORN) covering the Privacy Act information in this system. All sharing is compatible with the purpose for which the information was originally requested.

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

Information in CLAIMS 4 is tightly controlled and access is granted only to individuals with a specific need to access the system in order to perform their duties. Each transmission of data from CLAIMS 4 to an internal or external system is covered by an Interface Control Document (ICD) that describes the interface, levels of authentication and access control needed, data to be shared, and format and syntax of the data passing through the interface. The ICD also describes the security controls that protect the interface.

External entities do not have uncontrolled access to the CLAIMS 4 database. Once the data is shared, the receiving agency is responsible for assuring proper use of the data within its organization. All external sharing arrangements are covered by an appropriate routine use in the CLAIMS 4 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 4 sharing arrangements are consistent with existing routine uses or performed with the consent of the individual whose information is being shared. These routine uses limit the sharing of information from the system to the stated purpose of the original collection. In the N-400, applicants are advised that USCIS may provide information from their application to other government agencies. This sharing is memorialized in public Privacy Act systems of records notices on

which the public is allowed to comment. As required by DHS procedures and policies, all CLAIMS 4 routine uses are consistent with the original purpose for which the information was collected. These routine uses and public notices of CLAIMS 4 information use are reflected in limitations placed on all external sharing arrangements.

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 naturalization are presented with a Privacy Act Statement[5] and a release authorization on the N-400. The Privacy Act Statement details USCIS's authority to collect the information requested and how the information provided in the N-400 will be used by USCIS to process the application. The N-400 also contains a provision by which an applicant authorizes USCIS to release any information received from the applicant as needed to determine eligibility for naturalization.

Additionally, an updated System of Records notice is being published concurrently with this PIA.

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

Providing information on the N-400 is a voluntary act on the part of the individual seeking naturalization. The individual, however, must submit a complete application in order to complete the naturalization process. Applicants may decline to provide the required information; however, it may result in the denial of the application. This condition is clearly stated in the N-400.

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

The N-400 requires that applicants must complete all data fields in the application. This includes the submission of biometric information such as fingerprints, photographs, and signatures. This information is critical in making an informed decision regarding naturalization. The failure to submit such information prohibits USCIS from processing and properly adjudicating the application and thus precludes the applicant from obtaining naturalization. Therefore, during the application process, individuals consent to the use of the information submitted for adjudication purposes, including a background investigation. Specifically, the N-400 includes a Privacy Act Notice and requires the applicant's signature authorizing "the release of any information from my records that USCIS needs to determine eligibility for the benefit." The N-400 instructions further notify the applicant that "[USCIS] may provide information from your application to other government agencies."

---

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

This information is also conveyed in the SORN for this system and the Privacy Act Statement on the application itself. The information conveyed in the SORN is consistent with the information provided in this PIA. 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.

Risk: That applicants will not be aware of the purposes to which their information is put.

Mitigation: Applicants for naturalization are made aware that the information they are providing is being collected to determine whether they are eligible for naturalization. The N-400 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 via routine uses that describe the manner in which PII will be shared externally. In the USCIS Privacy Notice,[6] individuals are also notified that electronically submitted information is maintained and destroyed according to the requirements 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 on USCIS forms used to collect 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 a Privacy Act amendment requests. Any individual seeking to access information maintained in CLAIMS 4 should direct his or her request to USCIS National Records Center (NRC), P. O. Box 648010, Lee's Summit, MO 64064-8010. 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 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.

---

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

Requests for access to records in this system must be in writing. Such requests may be submitted by mail or in person. If a request for access is made by mail, the envelope and letter must be clearly marked "Privacy Access Request" to ensure proper and expeditious processing. The requester should provide his or her full name, date and place of birth, and verification of identity (full name, current address, and date and place of birth) in accordance with DHS regulations governing Privacy Act requests (found at 6 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 4 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.

When an applicant is interviewed by a USCIS adjudicator, the applicant also has the opportunity to make changes to his or her information in CLAIMS 4.

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 the deployment of Privacy Act exemptions or limited avenues for seeking redress and amendment of records.

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?

In compliance with federal law and regulations, users have access to CLAIMS 4 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 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 is established.

Criteria, procedures, controls, and responsibilities regarding CLAIMS 4 access are contained in the Sensitive System Security plan for CLAIMS 4. Additionally, there are several department and government-wide regulations and directives, which provide additional guidance and direction.

8.2 Will Department contractors have access to the system?

Contractors maintain CLAIMS 4 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 the system access application process (see Section 8.4) and been granted appropriate access levels by a supervisor are assigned a login ID and password to access the system. These users must undergo federally approved clearance investigations and sign appropriate documentation to obtain the appropriate access levels. Contractors are also required to sign non-disclosure agreements

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

All employees processing N-400 applications must successfully complete training on naturalization quality control procedures and training on the N-400 SOPs prior to performing any N-400 processing functions. Quality control procedures and SOPs are strict data quality processes that protect privacy by ensuring the accuracy and integrity of data input into CLAIMS 4. Only authorized trainers are allowed to conduct naturalization quality control training. Qualified contractor personnel conduct SOP training.

Additionally, all federal employees and contractors are required to complete annual Privacy Act and computer security awareness training.

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

In December of 2003, CLAIMS 4 obtained Authority to Operate (ATO) after completing DHS C&A requirements. A grant of ATO means that 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 system owner believes that the system should be allowed to operate. 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. The system is currently undergoing recertification. CLAIMS 4 has been classified as a "high" system and controls implemented in accordance with the Federal Information Security Management Act (FISMA) and National Institute for Standards and Technology (NIST) requirements.

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

When privileges expire (e.g., failure to change passwords every 90 days), user access is terminated automatically. Upon termination of employment at USCIS, managers are required to immediately seek the termination of the user's privileges. 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 4 also records Workflow Activities 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 4 service centers are required to follow USCIS application intake Standard Operating Procedures (SOPs). Corresponding audits ensure that local processes and procedures are consistent across the enterprise. Within CLAIMS 4 there are many business rules that ensure data integrity and consistency.

Remote access to CLAIMS 4 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 4, 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 limit access to the system to the minimum necessary. Audit trails are

kept in order to track and identify any unauthorized changes to information in the system. CLAIMS 4 has 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 4 complies 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 a CLAIMS 4 system is modified, the security engineers review the proposed changes and if required, perform a 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 4 is a case tracking system.

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

CLAIMS 4 is in 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 4 only contains information related to the application and adjudication of benefits. The system does not have the technology or the ability to monitor the activities of individuals or groups beyond that required to adjudicate applications. Approval Signature Page

Approval Signature

Original signed and on file with the DHS Privacy Office.

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