Privacy Impact Assessment
for the

Reengineered Naturalization Casework System

August 24, 2009

Contact Point
Donald Hawkins
Privacy Officer
United States Citizenship and Immigration Services
Department of Homeland Security
202-272-1400

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

Abstract

The Reengineered Naturalization Application Casework System (RNACS) is an electronic tracking system implemented at various United States Citizenship and Immigration Service (USCIS) offices to process and track applications associated with naturalization and/or citizenship. USCIS is conducting this Privacy Impact Assessment (PIA) because RNACS contains personally identifiable information (PII).

Overview

RNACS was originally developed to meet the information and case management needs of Immigration and Naturalization Service (INS) staff in headquarters, service processing centers, and the Citizenship Branch in district and regional offices. RNACS now supports USCIS' mission by expediting the completion of naturalization application processing, facilitating the management of the naturalization program, assuring uniformity in processing, supporting status queries on naturalization cases nationwide, and producing integrated management and statistical reports on all naturalization casework. RNACS was developed as an interim system to support naturalization processing in the period between the termination of Naturalization Application Casework System and the deployment of a replacement system.[1]

RNACS tracks applicants through the naturalization (N-400, *Application for Naturalization*) and citizenship (N-600, *Application for Citizenship*) processes from initial data entry through issuance of citizenship/naturalization documents. It also tracks and processes Applications for Replacement Naturalization/Citizenship Documents (N-565).[2] Since April 2001, no new N-400 cases have been entered into RNACS; all new N-400 cases are entered into Computer Linked Application Information Management System 4 (CLAIMS 4). RNACS users continue to process and close out the old N-400 cases. RNACS still accepts and processes N-565 and N-600 cases. Computer Linked Application Information Management System 3 (CLAIMS 3) intakes N-600s, but does not adjudicate.[3]

RNACS has two primary components: (1) an online data entry system, and (2) a system of batch programs that process casework, extract data, produce reports, and support interfaces with other systems.

Online Data Entry

The RNACS online system provides users with the ability to initially enter and track applications filed for citizenship or replacement certificates from the beginning of the process through adjudication and certificate printing. Through the online data entry system, USCIS employees manually run inquiries on naturalization and citizenship cases, update case information, and request reports. RNACS provides full case tracking and management capability for naturalization casework including assigning cases to Case Control Offices (CCO), queuing cases for appropriate actions, scheduling interviews and oath ceremonies, editing

[1] The Computer Linked Application Information Management System (CLAIMS 4) was intended to be the replacement system for tracking the N-400, *Application for Naturalization*.

[2] An applicant will fill out an N-565 if they have been issued a Naturalization Certificate, Certificate of Citizenship, Declaration of Intention or Repatriation Certificate which has been lost, mutilated, or destroyed; or if their name has been changed by marriage or by court order after the document was issued, and they seek a document in the new name. If they are a naturalized citizen desiring to obtain recognition as a citizen of the United States by a foreign country, they may apply for a special certificate for that purpose.

[3] For a full discussion of the CLAIMS 3 process, please see the Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum PIA at:
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_claims3.pdf.

all batch and online transactions to prevent erroneous or untimely case updates, producing scheduled reports (daily, weekly, monthly) and on-demand statistical and management reports, and producing user correspondence — application receipt acknowledgment, interview, re-interview and oath ceremony notices. RNACS maintains biographical and case data on naturalization applicants and a status history of all significant case updates. In addition, RNACS produces correspondence to applicants and their representatives including naturalization/citizenship certificates and notices for the applicants and their attorneys. RNACS produces mailers to inform those applicants and their representatives of scheduled appointments and of decisions made regarding their cases.

Batch Programs

In addition to RNACS's online capabilities, a number of regularly scheduled production batch jobs are run on the database. A batch job involves the programming of a system to perform a particular operation automatically on a group of files at the same time rather than manually performing the same functions on each file one file at a time. These jobs process casework (e.g., interview and other ceremony scheduling, batch certificate processing), generate reports, create files for updating other systems, launch the interfaces, and electronically update RNACS cases with data from interfaces with other systems.

Typical Transaction

A typical transaction begins when USCIS users enter the N-600 (the Citizenship form) or N-565 (Application for Replacement Naturalization/Citizenship Document) application data into RNACS. (As noted above, for N-400 applications received after 2001, data is entered directly into CLAIMS 4.) Data is entered from these forms to track applicants through the process of requesting a replacement certificate or for those applicants applying for citizenship. Once the application is complete, the USCIS user processes the application and makes a benefit determination. For the N-400 cases entered prior to April 2001, RNACS users may continue to process these cases through adjudication. See Appendix A for a complete discussion of the Citizenship, Naturalization, and Replacement of Documentation processes.

The legal authority for RNACS is derived from 8 United States Code (U.S.C.) §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.

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?

RNACS contains the following personal data elements obtained from the N-400, N-600, and N-565 applications:

Names: Name (last, first, middle, suffix) and name change, if applicable.

Address: Mailing address and resident address.

Personal Data: Date of birth, Social Security Number (SSN), gender, education, marital status, and applicant height.

Immigration Status Information: Naturalization date, year citizenship obtained, date of entry, port of entry, A-number, and immigration status.

Citizenship/Nationality Information: Country of birth, nationality, and place of birth.

Background Check Information: Response code on name check from the Federal Bureau of Investigation (FBI), Custom and Border Protection (CBP) TECS batch date (date TECS response returned), and TECS secondary check (if secondary check has been performed on case). Fingerprint responses from IDENT.

Naturalization Data: Naturalization certificate number, group A-number (owner), group form number, oath ceremony date, oath ceremony scheduled time, Naturalization Verification (Citizenship Naturalization Date/Time), Naturalization Verification (Citizenship Certificate Identification).

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

Most of the information in RNACS comes 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 fingerprint results[4] retrieved from FD-258,[5] response codes created during an FBI Name Check, TECS batch date (date TECS background check response is returned), and TECS secondary check (if secondary check has been performed on a particular case) are derived from those systems.[6]

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

USCIS collects this information in order to process and track applications associated with naturalization and/or citizenship. All information collected from applicants seeking benefits via applications that are processed by RNACS 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 RNACS to expedite the processing of the application or petition, to help ensure equitable treatment of applicants, to comply with legislative mandates, and to ensure the proper implementation of agency policies and regulations.

[4] The FBI Name Check provides information relating to the file the FBI has on the applicant if one exists. The FBI will furnish a response of NO RECORD, or POSITIVE RESPONSE which means the FBI has information relating to the name submitted.

[5] The FD-258 EE is an Oracle database table that stores the FBI Responses relating to send requests submitted through the USCIS Service Centers.

[6] For a detailed discussion on the FBI Name Check and TECS Background Check, please see *Privacy Impact Assessment for the USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum* (September 5, 2008), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_claims3.pdf.

1.4 How is the information collected?

USCIS employees manually enter most of the information in RNACS. This information is provided by the applicant on the following forms: N-400, *Application for Naturalization* (OMB No. 1615-0052), N-600, *Application for Certificate of Citizenship* (OMB No. 1615-0057), and N-565, *Application for Replacement Naturalization/Citizenship Document* (OMB No. 1615-0091).

The remainder of the information in RNACS is received electronically from the FBI Name Check process (via the USCIS FBI Query System), IDENT, directly, and TECS via an interface with CLAIMS 4. RNACS passes a file to CLAIMS 4, CLAIMS 4 adds data from the CLAIMS 4 TECS check files, and returns the results to RNACS in a results file.[7]

1.5 How will the information be checked for accuracy?

After receiving applications, USCIS employees manually enter the data into RNACS. The screens are configured to edit the data using predefined editing rules prior to accepting the data. USCIS developed Standard Operating Procedures (SOPs) which include detailed quality control reviews that help to ensure that the data has been accurately entered. These SOPs include 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. 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 RNACS.

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 or field office 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. Please see Section 7.0 for a full discussion on redress procedures offered by USCIS.

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 RNACS comes from 8 U.S.C. §1101 *et seq* of the Immigration and Nationality Act. More specifically, 8 U.S.C. §1103 charges the DHS Secretary with the duty of administering and enforcing all laws relating to the immigration and naturalization of aliens. The DHS Secretary has delegated benefit bestowing duties to the USCIS Under Secretary pursuant to a departmental management directive. In addition, pursuant to the Paperwork Reduction Act, OMB has approved the content and format of every public form used by USCIS.

[7] For a detailed discussion on IDENT, please see Privacy Impact Assessment for the USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (September 5, 2008), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_claims3.pdf.

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 RNACS.

Mitigation: USCIS has mitigated this risk by developing separate, detailed SOPs for handling information collected in 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 RNACS. These procedures are designed to 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 RNACS and saved.

USCIS also mitigates this risk by allowing applicants to make changes to their information in RNACS 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 or field office where the application was filed and request correction. USCIS also allows the applicant to file a Privacy Act request to review and amend erroneous records.

Privacy Risk: There is a risk that the system may collect more information than 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 RNACS to that necessary to process or adjudicate the applications. USCIS designed RNACS to only collect specific data elements. 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 RNACS, USCIS limits the PII stored in the system 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 (PRA) collection reviews. USCIS also disposes of RNACS information promptly as required by the records retention schedule negotiated with the National Archives and Records Administration (NARA).

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 uses the PII in RNACS to establish the applicant's identity and history with USCIS; determine their eligibility for the benefit sought; expedite the processing of the application or petition; and help ensure equitable treatment of applicants, compliance with legislative mandates, and proper implementation of agency policies and regulations.

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

No tools are used to analyze the data in RNACS.

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

RNACS does not use commercially or publicly available data.

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: There is a risk that users who have access to RNACS will use the information in unauthorized manners.

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 RNACS). 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. Rules of Behavior are part of a comprehensive program to provide complete information security. These guidelines are established to hold users accountable for their actions and responsible for IT security. Rules of Behavior establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. OMB Circular A-130 requires that all major applications and general support systems have Rules of Behavior. RNACS users are required to read and sign the Rule of Behavior prior to receiving access to the system. A record of those users who have signed is maintained by the ISSO. Disciplinary action can be taken for violating the Rules of Behavior. The RNACS Rules of Behavior conform with 4300A DHS Sensitive Security Handbook - Rules of Behavior.

Any person who is in non-compliance with the rules of behavior is subject to penalties and sanctions, including verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, criminal or civil prosecution, or termination, depending on the severity of the violation.

Users are presented the DHS guidelines for corporate Rules of Behavior when completing the mandatory security application for access to RNACS. Users acknowledge they have read, understood, and agreed to the content of these rules. These rules cover system access, passwords and other access control measures, data protection, use of government office equipment, software, internet and e-mail use, incident reporting, and accountability. They acknowledge, by signing and dating the DHS Rules of Behavior that violating the system rules of behavior will involve potential disciplinary actions.

Privacy Risk: Unauthorized users gain access to RNACS.

Mitigation: All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards that include restricting access to authorized personnel who have a need-to-know. Access to RNACS is given only to a limited number of users for the purpose of determining benefit eligibility. Users must use their issued credentials to gain access to the system. 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?

Electronic data located in RNACS will be deleted or destroyed 15 years after the last completed action (N1-566-08-15). The 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.

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

NARA approved the retention schedule on August 28, 2008.

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

Privacy Risk: There is a risk that RNACS data could be maintained for a period longer than necessary to achieve agency's mission.

Mitigation: Although there is always risk inherent in retaining personal data for any length of time, the RNACS data retention period identified in the NARA schedule is consistent with the concept of retaining personal data only for as long as necessary to support the agency's mission. NARA has approved the RNACS schedule.

Privacy Risk: Because some of the cases located in RNACS predate the creation of USCIS, there is a risk that some of the information in RNACS may no longer be accurate.

Mitigation: USCIS does not currently review cases predating USCIS, but relies on the accuracy of the information when originally entered. Further, newly issued USCIS policies relating to the naturalization functions have not altered the data accuracy standards post USCIS creation.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

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

Information in RNACS is shared with the following internal systems/components:

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. RNACS users use an online function to request the transfer of A-Files from CIS and updates CIS with the status of naturalization cases.

Computer-Linked Application Management System 3 Mainframe (CLAIMS 3/MF): CLAIMS 3/MF is a mainframe database centered major application that supports processing of USCIS applications and petitions for various immigrant benefits (e.g., change of status, employment authorization, extension of stay, etc). It supports case management for and adjudication of all USCIS benefits except naturalization and citizenship. CLAIMS 3/MF sends case receipt data and employment authorization data derived from USCIS Forms N-565 and N-600 to RNACS.

Computer-Linked Application Management System 4 (CLAIMS 4): CLAIMS 4 is the USCIS system for processing Applications for Naturalization. RNACS is one of the systems of records for N-400 cases, so N-400 cases entered into CLAIMS 4 are uploaded into RNACS. 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, and current status) to RNACS electronically over the USCIS Mainframe. Prior to April 2001, N-400 cases were entered directly into RNACS.

Verification Information System (VIS): VIS is a composite information system incorporating data from various DHS databases. It is the underlying information technology that provides immigration status verification for 1) benefits determinations through the Systematic Alien Verification for Entitlements (SAVE) program for government benefits and 2) verification of employment authorization for newly hired employees through the E-Verify program. VIS uses the Enterprise Service Bus (ESB) to read information in the RNACS database. The ESB consists of various off-the-shelf commercial products that work together to provide an easy to use interface.

Receipt and Alien File Accountability and Control System (RAFACS): RAFACS is the file management system in use at USCIS service centers and most local offices. The RNACS interface with RAFACS allows checks to determine whether a particular A-File is present at a processing site. If not, the files are retrieved through CIS online transfer requests and cases are held until the files arrive on-site. RNACS users are able to query RAFACS for the location of A-Files onsite at any stage of naturalization processing. RAFACS is also used for (1) generating reports in responsible party code order, which is a

mechanism used to disseminate reports within the local office and (2) batch certificate printing, which is a process that allowed the office to select a group of cases and have certificates printed for those cases in lieu of selecting and printing them one at a time.

DHS CBP TECS: After USCIS completes a TECS background check search, RNACS receives and stores information indicating whether the TECS query returned a response indicating that there was no information about the applicant in the TECS system. If the TECS query returns a response indicating that there is information in the TECS system, no notation is made in RNACS. The authorized TECS 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.

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, or disclosure of, information contained within RNACS.

Mitigation: 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 RNACS 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?

Applicant information contained in RNACS (name, date of birth, country of birth, race and gender) is sent to the FBI in order to conduct the 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. 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's 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 RNACS. 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 or No Record). RAP sheets are not stored in RNACS.

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.

Information in RNACS is covered by the Benefits Information System (BIS) Systems of Records Notices (SORN) (DHS-USCIS-007, September 29, 2008 73 FR 56596) and its applicable routine uses. Specifically, BIS information may be shared with law enforcement authorities in the proper conduct of their mission and duties and pursuant to a law enforcement investigation.

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

Information in RNACS is tightly controlled and access is granted only to individuals with a specific need to access the system in order to perform their duties. External entities do not have access to the RNACS database. For the purposes of the information sharing with the FBI, once the data is shared, the receiving agency is responsible for assuring proper use of the data within its organization. The FBI sharing arrangement is covered by an appropriate routine use in the BIS 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: The FBI sharing arrangement is 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, N-600, and N-565, applicants are advised that USCIS may provide information from their application to other government agencies. This sharing is memorialized in public Privacy Act SORNs which the public is allowed to comment. As required by DHS procedures and policies, all RNACS routine uses are consistent with the original purpose for which the information was collected. These routine uses and public notices of RNACS 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?

USCIS provides Privacy Act notice on all immigration forms. The following language is found on the three forms used in RNACS data entry:

> *We ask for the information on this form and for other documents to determine your eligibility for naturalization. Form N-400 processes are generally covered in 8 U.S.C. §§ 1421 through 1430 and 1436 through 1449. We may provide information from your application to other government agencies.*
>
> *USCIS will use the information and evidence requested on Form N-600 to determine your eligibility for the requested immigration benefit. We may provide information from your application to other government agencies.*
>
> *We ask for the information on this form, and associated evidence, to determine if you have established eligibility for the immigration benefit for which you are filing. Our legal right to ask for this information can be found in the Immigration and Nationality Act, as amended. We may provide this information to other government agencies. Failure to provide this information, and any requested evidence, may delay a final decision or result in denial of your Form N-565.*

Additionally, the BIS SORN and this PIA provide notice to individuals regarding the manner in which their information will be used.

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

Providing information on the N-400, N-600, and N-565 is a voluntary act on the part of the

individual seeking the benefit. The individual, however, must submit a complete application in order to complete the 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 forms.

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 forms require that applicants must complete all data fields in the application. This information is critical in making an informed decision regarding immigration benefits. The failure to submit such information prohibits USCIS from processing and properly adjudicating the application and thus precludes the applicant from obtaining benefits. Therefore, during the application process, individuals consent to the use of the information submitted for adjudication purposes. Specifically, the forms include a Privacy Act Notice and require the applicant's signature authorizing "the release of any information from my records that USCIS needs to determine eligibility for the benefit." The form instructions further notify the applicant that "[USCIS] may provide information from your application to other government agencies."

This information is also conveyed in the BIS SORN 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.

Privacy Risk: Applicants may not be aware of the purposes for which their information is collected.

Mitigation: Applicants are made aware that the information they are providing is being collected to determine whether they are eligible for benefits. The forms contain 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 BIS 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,[8] 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.

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

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 RNACS 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 (C.F.R.) § 5.21.

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

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

The BIS SORN 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.

Privacy 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 C.F.R. § 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?

Users must fill out G-872A and G-872D and submit it to the Password Issuance and Control (PICS) Office of USCIS for access to RNACS. After a user receives his PICS ID, the local PICS security officer creates an internal RNACS access profile record. The security officer discretely grants access to RNACS based upon the user's job role. The lowest levels of access are inquiry-only functions. These include case inquiry, including history actions and name/date-of-birth inquiry, as well as other inquiry-only commands. Non-RNACS users are not authorized anything higher than inquiry commands. Users can be granted access to case update (N-400, N-565, and N-600), examination results, oath ceremony closeout, and various other sensitive commands as required. Extremely sensitive commands such as case denaturalization require Program Management approval and a special registration.

8.2 Will Department contractors have access to the system?

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 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 applications must successfully complete training on naturalization quality control procedures and training on the application's SOPs prior to performing any 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 RNACS. 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 been completed for the system or systems supporting the program?

The RNACS Authority to Operate (ATO) expires on July 31, 2011.

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

RNACS data is secured through password control at the transaction level for each user. Passwords are controlled through the PICS, which is directly fed by the personnel roster, providing regular updates on personnel changes. Security is also provided by DHS hiring practices and personnel background checks.

USCIS supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls. RNACS uses the existing security measures implemented by the mainframe systems it accesses.

RNACS writes history records for case update activity on a case-by-case basis. The history record shows the specific user ID or batch program, and the activity and date the activity was performed. These history records can be viewed using the case status (CASE) command.

User activities are also reviewed through the use of Integrated Database Management System (IDMS)/R journal logs. The ISSO reviews these activity logs periodically.

Remote access to RNACS is restricted to secure methods employing approved identification and authentication as well as intrusion detection and unauthorized access monitoring. Controls are in place via the Nortel Network's Contivity VPN Client Monitor to ensure that remote users are positively identified and authenticated before connection is authorized. Authentication methods include use of the SecurID password generated every minute for each RNACS maintenance person, enabled logging, and 128-bit encryption.

Remote access, download, and the storage of PII information is permitted (after approval by the DAA prior to implementation). PII collected, processed, and maintained by the system cannot be physically removed from the USCIS without the written permission of the system owner. Users with the ability to remotely access, download, and store data must have a valid VPN token/SecurID issued by USCIS Office of

Information Technology and a government furnished laptop equipped with the appropriate encryption software (as described above). Those users with remote access have been trained on the requirements for protecting sensitive information. In all instances, access to this data is restricted to authorized personnel with a valid need to know to perform their job responsibilities.

Dial-up connections are restricted.

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 RNACS, 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. RNACS 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, RNACS complies with DHS and Federal Information Security Management Act (FISMA)/ National Institute of Standards and Technology (NIST) security requirements, which provide criteria for securing networks, computers, and computer services against attack and unauthorized information dissemination. Each time RNACS 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 and Privacy Act 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, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

RNACS is a centralized IDMS.

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

RNACS is currently in the Operational and Maintenance (O&M) phase of the System Development Life Cycle Methodology.

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

RNACS 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

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix A

Citizenship Process

In order to begin the process to acquire citizenship, an individual must complete Form N-600. Form N-600 may be filed by any person claiming to have acquired (at birth) or derived (after birth) U.S. citizenship through a parent who is a U.S. citizen. Upon completion, the applicant submits the application to the district or field office for his or her region. Along with the completed application, the applicant must submit the following, where applicable: two color photographs, a copy of his or her birth certificate, marriage certificate and copy of termination of marriage, proof of the parent's U.S. citizenship such as a copy of a N-550, Certificate of Naturalization, proof of status as a national of the United States, proof of legitimacy, proof of legal custody, copy of Permanent Resident Card or other evidence of Lawful Permanent Resident status, proof of required residence or physical presence in the United States (e.g., deeds, mortgages, or employment records), copy of full final adoption decree, and evidence of legal name changes. If it is not possible to obtain one of the above listed documents, USCIS may accept a certificate under the seal of the church where a baptism occurred, showing the date and place of the child's birth, date of baptism, the names of the godparents, if known, a certificate under the church seal issued within two months of birth or a letter from authorities of the school attended (preferably the first school), showing the date of admission to the school, the child's date of birth or age at that time, place of birth, and the names and places of birth of parents, if shown in the school. RNACS only records the date of birth and the country of birth.

Once a Form N-600 has been accepted, it is checked for completeness, including submission of the required initial evidence. If the applicant does not completely fill out the form, or files it without required initial evidence, he or she may not establish a basis for eligibility, and USCIS may deny his or her Form N-600. USCIS may request more information or evidence, or may request that the applicant appear at a USCIS office for an interview. USCIS may also request that the applicant submit the originals of any copy. USCIS returns these originals when they are no longer required. The decision on a Form N-600 involves a determination of whether the applicant has established eligibility for the requested benefit. Once the USCIS employee determines the benefit, USCIS sends notice of the decision in writing to the applicant.

Naturalization Process

In order to begin the naturalization process, an individual must complete Form N-400. 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, 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.

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 some[9] of the applicant's information from the form into the CLAIMS 4[10] server at the service center. After USCIS personnel enter information from the application into the system, USCIS sends

[9] The data elements are discussed in detail in section 1.0.
[10] Since April 2001, no new N-400 cases have been entered into RNACS; all new N-400 cases are entered into Computer Linked Application Information Management System 4 (CLAIMS 4).

an appointment letter to the applicant indicating when and where the applicant must go to submit biometric and biographic data needed to complete the process.

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 Biometric Benefits Support System (BBSS).

After the fingerprints are taken, the applicant must wait for USCIS to schedule a personal interview. The ASC sends this data via the 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 Federal Bureau of Investigation (FBI) where the background checks are conducted. Biographic and biometric data collected 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 PII with the FBI and DHS Customs and Border Protection (CBP) to conduct name-based and fingerprint-based criminal history background checks.

Replacement of Naturalization or Citizenship Document Process

There are three circumstances in which an applicant may fill out an N-565:

1. If the applicant has been issued a Naturalization Certificate, Certificate of Citizenship, Declaration of Intention, or Repatriation Certificate that has been lost, mutilated, or destroyed.

2. If the applicant's name has been changed by marriage or by court order after the document was issued and the applicant seeks a document in the new name.

3. If the applicant is a naturalized citizen desiring to obtain recognition as a citizen of the United States by a foreign country. The applicant may apply for a special certificate for that purpose.

The applicant must complete the N-565 form and provide two copies of a photograph taken within 30 days of the N-565 submission. In addition, the applicant must submit the mutilated document, if applicable, the original USCIS Naturalization or Citizenship document, a copy of a marriage certificate (if a name change), and a copy of the naturalization certificate, if applying for a special certificate.

If the applicant resides in AL, AR, CT, DE, DC, FL, GA, KY, LA,MS, ME, MD, MA, NH, NJ, NM, NY, NC, SC, OK, PA,PR, RI, TN, TX, VA, VI, VT, WV, he or she must submit the N-565 to the Texas Service Center. If the applicant resides in AK, AZ, CA, CO, GU, HI, ID, IL, IN, IA,KS, MI, MN, MO, MT, NE, NV, ND, OH, OR, SD, UT,WA, WI, WY, he or she must submit the N-565 to the Nebraska Service Center.

Once the application has been accepted, it is checked for completeness, including submission of the required initial evidence. USCIS may request additional information from the applicant and/or may

require that the applicant appear at a USCIS office for an interview. USCIS may also request that the applicant submit the originals of any copy. USCIS returns these originals when they are no longer required. If the applicant establishes eligibility for the benefit, his or her application is approved and the appropriate document is issued. Under certain circumstances, a special certificate of naturalization will be forwarded to the U.S. Department of State (DoS) for delivery to a foreign government official. If the application is denied, USCIS notifies the applicant in writing of the reasons for the denial.