



**Privacy Impact Assessment Update
for the**

Computer Linked Application Information Management System

DHS/USCIS/PIA-015(a)

August 31, 2011

Contact Point

Donald Hawkins

Privacy Officer

United States Citizenship and Immigration Services

(202) 272-8000

Reviewing Official

Mary Ellen Callahan

Chief Privacy Officer

Department of Homeland Security

(703) 235-0780



Abstract

The United States Citizenship and Immigration Services (USCIS) is publishing this update to the Privacy Impact Assessment (PIA) for the Computer Linked Application Information Management System (CLAIMS 4) dated September 5, 2008.¹ CLAIMS 4 is an electronic case management system used to track and process applications for naturalization. The purpose of this update is to: (1) discuss the disposition of the Change of Address (CoA) subsystem; (2) discuss the disposition of the Complete File Review (CFR) subsystem; (3) describe the new privacy impacts associated with the exchange of zip codes between the Site Profile System (SPS) and CLAIMS 4; (4) describe the new privacy impacts associated with the capturing of certain digitized biometric images through the Benefits Biometric Support System (BBSS); and (5) provide notice of a pilot program under which the Department of Homeland Security (DHS) is expanding the sharing of CLAIMS 4 data with the National Counterterrorism Center (NCTC) in support of DHS's mission to protect the United States from potential terrorist activities.

Introduction

The United States Citizenship and Immigration Services (USCIS) is responsible for the administration and adjudication of naturalization applications. To support the execution of its mission, USCIS implemented the Computer Linked Application Information Management System (CLAIMS 4) at various USCIS service centers to process and track naturalization applications through the adjudication process from the receipt of the application to benefit determination. CLAIMS 4 is an electronic case management system used for processing Form N-400, *Applications for Naturalization*. Its functions include receipting, data entry, recording benefit determinations (e.g., approvals and denials), and other operations necessary to process naturalization applications.

USCIS is updating the CLAIMS 4 PIA dated September 5, 2008 to discuss how CLAIMS 4 no longer interfaces with its Change of Address (CoA) and Complete File Review (CFR) subsystems to exchange applicant information. The disposition of these subsystems was completed in November 2009. Further, this update describes CLAIMS 4 new interfaces and privacy impacts with the Site Profile System (SPS) and Benefits Biometric Support System (BBSS). A pilot program under which DHS is expanding the sharing of CLAIMS 4 data with the National Counterterrorism Center (NCTC) in support of DHS's mission to protect the United States from potential terrorist activities is also described in this update.

Decommissioning of Subsystems

Change of Address

USCIS decommissioned the Change of Address (CoA) subsystem, which allowed N-400 applicants to submit change of address requests over the phone. Previously, applicants called the USCIS National Customer Service Center (NCSC) to report a new address. This information was then entered

¹ The CLAIMS 4 PIA (DHS/USCIS/PIA-015) is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_claims4.pdf.



into the service center application, which automatically updated CoA with the new information. CoA then electronically transferred the information to CLAIMS 4 and the Reengineered Naturalization Application Casework System (RNACS) to update the applicant's information. The purpose of CoA was to update CLAIMS 4 and RNACS with the applicant's updated address.

USCIS continues to collect new address information from naturalization applicants telephonically. However, USCIS altered the technology used to capture address changes for naturalization applicants. Currently, when an applicant calls the USCIS NCSC to report an address change, the Customer Service Representative (CSR), after verifying the applicant's identity through asking a series of questions based off applicant data, records the new information in the Customer Relationship Interface System (CRIS)² Service Request Management Tool (SRMT). CRIS SRMT is a "tool set" used by USCIS to handle specific service requests. The following information is collected from the applicant: full name, date of birth (DOB), country of birth, phone number, alien number, where the N-400 application was submitted, former residential and/or mailing address, and new residential and/or mailing address. A CLAIMS 4 user then manually updates the address information in the CLAIMS 4 Address Change Petition module. All change of address notifications received via the phone are entered directly into this module, which replaced CoA. CoA currently resides in the CLAIMS 4 database.

Complete File Review

Complete File Review (CFR), a subsystem to CLAIMS 4, was developed to allow adjudicators at each service center to review the contents of a naturalization application in order to ensure all necessary supporting documents were submitted. CFR imported the following biographic data about the naturalization applicant from CLAIMS 4: full name (first, middle, and last), mailing address, DOB, aliases, and gender. To review the application for completeness, adjudicators used the information in the naturalization application, the Alien File (A-File), and the Federal Bureau of Investigation (FBI) fingerprint results and identified any missing documentation that would be required by adjudicators to determine whether to grant or deny the application. This subsystem assisted USCIS adjudication staff in ensuring that all necessary documentation required for N-400 applicants was submitted prior to their interview, thus reducing costly and time-consuming delays.

USCIS decommissioned the CFR subsystem due to a drastic reduction in use resulting from the shift of initial application reviews from the four service centers to the National Benefits Center (NBC). NBC was established to serve as the hub and conduit to accomplish N-400 pre-interview processing. NBC found that file review methodologies developed in-house often suited their needs more efficiently than the CFR application. CFR no longer collects or stores information derived from CLAIMS 4. CFR currently resides in the CLAIMS 4 database.

² The CRIS PIA (DHS/USCIS/PIA-019) is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_crisupdate.pdf.



Introduction of New Systems

Site Profile System

The Site Profile System (SPS) is a new system that includes USCIS Application Support Center (ASC) location, contact, personnel, and equipment information. SPS also assists USCIS with determining which USCIS ASC should handle a particular geographic area based on zip codes. SPS sends these zip code assignments directly to CLAIMS 4, from which applicants are assigned to a particular ASC for interview scheduling based on their residential address.

SPS provides USCIS with the ability to more efficiently manage workload, optimize operations, and improve the use of administrative time. Upon becoming aware of new or updated zip codes through the United States Postal Service, USCIS may change a zip code assignment from one ASC to another ASC to balance appointment workload. SPS also supports the workload management of the CLAIMS 4 and Scheduling and Notification of Applicants for Processing (SNAP) major applications by providing ASC managers with input and reporting capabilities. For example, ASC managers may extract and compile data from CLAIMS 4 and SNAP to view consolidated appointment schedules and backlog for each ASC.

Benefits Biometrics Support System

USCIS redesigned the Certificate of Naturalization as part of the Naturalization Certificate Automation and Redesign (NCAR) initiative. Previously, USCIS required the applicant to submit two passport-style photographs along with his or her application for naturalization. If the application for naturalization was approved, one of the hard copy photographs of the applicant was affixed to the naturalization certificate. The other hard copy photograph was retained in the applicant's application file. USCIS also required the applicant to sign the naturalization certificate at the time the naturalization certificate was issued.

In order to adopt the latest physical security features under NCAR, which are aimed at deterring fraud and improving the quality and integrity of the immigration system, USCIS modified the procedures for capturing the applicant's photograph and signature onto the naturalization certificate. In addition to the requirement for the applicant to submit passport-style photographs along with his or her naturalization application, USCIS now requires the collection of a digitized photograph and digitized signature from the applicant. If the application for naturalization is approved, these digitized biometric images are transferred from BBSS to CLAIMS 4 and embedded into the naturalization certificate prior to issuance.

Information Sharing with NCTC

Under a pilot program, DHS is expanding its sharing of CLAIMS 4 data with NCTC in support of DHS's mission to protect the United States from potential terrorist activities. Pursuant to the National Security Act of 1947, as amended, NCTC "serve[s] as the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support (50 U.S.C. § 404o)." In order to enhance information sharing, the President issued Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to*



Protect Americans (October 27, 2005), which provides that the head of each agency that possesses or acquires terrorism information shall promptly give access to that information to the head of other agencies that have counterterrorism functions. The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 (Pub. L. No. 108-458), as amended, places an obligation on U.S. government agencies to share terrorism information with the intelligence community. In such instances, DHS may share the entire dataset with an intelligence community member in order to support the counterterrorism activities of the intelligence community and to identify terrorism information within DHS data.

Under a Memorandum of Understanding (MOU) between DHS and NCTC, DHS may share non-naturalized citizen information maintained in the CLAIMS 4 database with NCTC. The MOU permits NCTC to use CLAIMS 4 information to facilitate NCTC's counterterrorism efforts. This information sharing also aligns with DHS's mission to prevent and deter terrorist attacks. The MOU includes a number of safeguards to ensure the data is only used for the purposes explicitly permitted under the MOU, this PIA update, and the DHS/USCIS-007 Benefits Information System (BIS) System of Records Notice (SORN) (September 29, 2008, 73 FR 56596). The MOU also limits the retention period that NCTC may maintain the data, ensures proper information technology security is in place during and after transmission of the data to NCTC, requires training on interpreting CLAIMS 4, and provides for routine reporting and auditing of NCTC's use of the data.

Reason for the PIA Update

DHS and USCIS are updating the CLAIMS 4 PIA, first published on September 5, 2008, to reflect the disposition of the CoA and CFR subsystems and the new interfaces with SPS and BBSS.

Additionally, DHS and USCIS are updating the CLAIMS 4 PIA to account for the sharing of CLAIMS 4 data with NCTC in support of the Department's mission to protect the United States from potential terrorist activities. DHS has entered into a MOU with NCTC in order to facilitate NCTC's counterterrorism efforts. This information sharing also aligns with DHS's mission to prevent and deter terrorist attacks. DHS and NCTC have placed specific safeguards in the MOU to ensure that the data is used appropriately and in accordance with this PIA update and the DHS/USCIS-007 BIS SORN.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

The Systems and the Information Collected and Stored within the Systems

With this PIA update, CLAIMS 4 has decommissioned the collection and storage of information in the CoA and CFR subsystems. USCIS continues to collect change of address information. Section 265 of the Immigration and Naturalization Act (INA) requires all naturalization applicants to report a change of address to USCIS within ten days of the change. USCIS NCSC allows naturalization applicants to report address changes to ensure their information is current and accurate. USCIS NCSC, after verifying the applicant's identity, inputs the applicant's new address into CRIS SMRT. The CLAIMS 4 user then updates the applicant's address in the CLAIMS 4 Address Change Petition module, which replaced CoA.



The change of address data previously stored in CoA is now maintained in CLAIMS 4. Also, all naturalization application data previously stored in CFR resides in the CLAIMS 4 database. CoA and CFR were properly sanitized before disposal to minimize the risk of unauthorized disclosure in accordance with DHS policy.

In addition, this PIA update reflects the collection of new zip code mapping data from SPS and the applicant's digital photo and signature from BBSS. As described in the Introduction section, CLAIMS 4 receives zip code mapping information from SPS. Zip code changes occur when there is a new zip code or if there is a change to zip code mapping to balance out the workload at the ASCs.

The CLAIMS 4 Biometric Retrieval Unit subsystem transfers the applicant's digital photo and signature from BBSS. The collection of this information provides USCIS with the capability to print the photograph and signature directly onto the naturalization certificate, thus provides CLAIMS 4 with modifications and enhancements to support the NCAR initiative. The changes for the enhanced production of the naturalization certificate include:

- Printing all naturalization certificates produced by CLAIMS 4 on the redesigned certificate stock;
- Printing the applicant's city, state, and/or country of residence on the naturalization certificate at the time of the applicant's oath ceremony (this information will be verified during the interview process);
- Printing digitized biometric images where the N-400 applicants appeared at the ASC and had digital images captured;
- Adding the USCIS Director's signature image to the CLAIMS 4 database for retrieval and printing on the naturalization certificate;
- Extending the data elements contained on the Oath Preparation and Declaration Form used by the adjudicator; and
- Viewing the digitized images by the adjudicator during the interview.

Uses of the System and the Information

USCIS continues to use CLAIMS 4 information to administer and adjudicate benefits for naturalization as described in Section 2.0 of the CLAIMS 4 PIA published on September 5, 2008.

New uses of information in CLAIMS 4 includes the use of zip codes for zip code mapping to facilitate the assignment of an applicant to a particular ASC for interview scheduling, as well as the use of the digitized photo and signature captured during the ASC appointment, which will be printed directly onto the naturalization certificate in support of the NCAR initiative.

Retention

The National Archives and Records Administration's (NARA) approved retention schedule [N1-563-04-04] has not changed. Records in CLAIMS 4 will be deleted 15 years after the application for naturalization is approved, 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, which is stored in the applicant's Alien File (A-File).



The A-File retention schedule [N1-566-08-11] has been updated and approved by NARA.³ Previous encounter information maintained in the A-file will now be retained in accordance with the A-file retention schedule, which is 100 years from the applicant's DOB; thereafter the file is retired to NARA as a permanent record.

Under a pilot program, DHS is expanding its sharing of CLAIMS 4 data with NCTC in support of DHS's mission to protect the United States from potential terrorist activities. Pursuant to an MOU, NCTC will be allowed to retain non-naturalized citizens data maintained in CLAIMS 4 for up to 180 calendar days of receipt in order to support the counterterrorism activities of the intelligence community and to identify terrorism information within DHS data. CLAIMS 4 data will be deleted by NCTC no later than 180 calendar days of receipt unless a nexus to terrorism has been identified for a particular record. NCTC may retain CLAIMS 4 data containing terrorism information in accordance with NCTC authorities and policies, applicable law, and the terms of the MOU.

Internal Sharing and Disclosure

USCIS is amending Section 4 of the CLAIMS 4 PIA to address a publishing error. In contrast to the CLAIMS 4 PIA published on September 5, 2008, CLAIMS 4 does not transmit change of address data to or from the USCIS systems associated with benefits processing of applicants other than petitions for naturalization, refugee status, and asylum (CLAIMS 3). The CLAIMS 3 and CLAIMS 4 interface is limited to the sharing of Form I-485 data for the purpose of scheduling interviews to adjudicate Form I-485, which is the Application to Register Permanent Residence or Adjust Status.

External Sharing and Disclosure

CLAIMS 4 will continue to share and disclose information with agencies external to DHS in support of the administration and adjudication of naturalization benefits as described in Section 5.0 of the CLAIMS 4 PIA.

In addition, DHS has entered into a new sharing agreement with NCTC in order to facilitate NCTC's counterterrorism efforts. Pursuant to 8 CFR 208.6(a), an exercise of the Secretarial disclosure authority has been signed to allow this sharing. This information sharing also aligns with DHS's mission to prevent and deter terrorist attacks. This sharing is conducted pursuant to routine uses G and U of the DHS/USCIS-007 BIS SORN, which states that DHS may share CLAIMS 4 information with a "Federal, State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities, when DHS reasonably believes such use is to assist in anti-terrorism efforts, and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure."

NCTC will process all CLAIMS 4 data within 180 calendar days of receipt from DHS to determine whether a nexus to terrorism exists. NCTC will immediately purge all CLAIMS 4 data that does not constitute terrorism information no more than 180 calendar days from receipt. This process will be audited as required under the MOU. NCTC will review, retain, and disseminate CLAIMS 4 data that it

³ See the DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking SORN (June 13, 2011, 76 FR 34233) <http://www.gpo.gov/fdsys/pkg/FR-2011-06-13/html/2011-14489.htm> for additional information.



has determined to have a nexus to terrorism in accordance with procedures under the Memorandum of Agreement between the Attorney General and the Director of National Intelligence on *Guidelines for Access, Retention, Use and Dissemination by the NCTC of Terrorism Information Contained within Datasets Identified as Including Non-terrorism Information and Information pertaining Exclusively to Domestic Terrorism*, November 2008, Section 2.3 of Executive Order 12333, and additional terms specified in the MOU.

As described in the MOU, strict safeguards are in place to protect the data provided to NCTC. These protections include a routine oversight of NCTC's use of the data by DHS personnel detailed to NCTC. In addition, training has been provided to NCTC users on the appropriate use of personally identifiable information. DHS and USCIS will provide annual and periodic training to appropriate NCTC personnel on proper interpretation of the data contained in CLAIMS 4 and on proper treatment of data from certain categories that require special handling, such as asylum, refugee, U Visa, T Visa, and U.S. person data.

In general, NCTC may not share CLAIMS 4 data unless that data was identified as containing terrorism information and in accordance with the procedures described in the MOU. NCTC shall maintain an electronic copy of the CLAIMS 4 data that was disseminated, to whom it was disseminated, and the purpose for the dissemination. If there is a question on CLAIMS 4 data and its relationship to terrorism, NCTC may request permission from DHS to share this data with other intelligence agencies.

This external sharing is also being appropriately logged pursuant to subsection (c) of the Privacy Act, which requires the Department to maintain a log of when records have been shared outside of DHS.

Notice

There are no changes to notice procedures in the CLAIMS 4 PIA published on September 5, 2008.

Individual Access, Redress, and Correction

There are no changes to the access, redress, and corrections procedures identified in the CLAIMS 4 PIA published on September 5, 2008.

Technical Access and Security

The technical access and security controls for CLAIMS 4 have not changed. The new sharing is conducted in conformance with existing information technology security protocols including encryption. Please refer to the CLAIMS 4 PIA for more information.

Technology

USCIS decommissioned the CoA and CFR subsystems. The CoA subsystem was replaced by the Change of Address Petition module to capture change of address updates. The functions performed by CFR were assumed by NBC. CoA and CFR were decommissioned in accordance with DHS policy. SPS interfaces with CLAIMS 4 for zip code data mapping. BBSS transfers the applicant's digitized photograph and signature to CLAIMS 4 in support of the NCAR initiative.



Responsible Official

Donald Hawkins, Privacy Officer
United States Citizenship and Immigration Services
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security