



Privacy Impact Assessment
for the

Case and Activity Management for
International Operations (CAMINO)

DHS/USCIS/PIA-051

May 26, 2015

Contact Point

Donald Hawkins

Privacy Officer

United States Citizenship and Immigration Services

(202) 272-8000

Reviewing Official

Karen L. Neuman

Chief Privacy Officer

Department of Homeland Security

(202) 343-1717



Abstract

The Department of Homeland Security (DHS) U.S. Citizenship and Immigration Services (USCIS) developed the Case and Activity Management for International Operations (CAMINO) system to support the USCIS Refugee, Asylum, and International Operations Directorate's (RAIO) International Operations (IO) Division and, in certain cases, the Refugee Affairs Division (RAD). CAMINO is a secure, web-based, case management application designed to facilitate the processing of immigration applications and petitions received or adjudicated by RAIO IO. This Privacy Impact Assessment (PIA) discusses the USCIS system used to support RAIO IO and evaluates the privacy risks and mitigation strategies built into the system. USCIS is conducting this PIA because CAMINO collects and uses personally identifiable information (PII).

Overview

The U.S. Citizenship and Immigration Services (USCIS) Refugee, Asylum, and International Operations Directorate (RAIO), International Operations (IO) Division is charged with advancing the USCIS mission in the international arena. USCIS IO offices are located both overseas and domestically.¹ RAIO IO provides subject matter expertise on immigration-related matters, grants various immigration and citizenship benefits, and ensures the integrity of the U.S. immigration system for its overseas customers.

IO staff adjudicate a wide variety of petitions and applications (applications) and issue travel documents to overseas customers. In addition to assisting overseas applicants applying for travel documents to enter the United States, IO staff also assist:

- U.S. citizens, lawful permanent residents (LPR), asylees, and refugees who wish to bring relatives to the United States;
- Individuals who have been persecuted or fear persecution and wish to resettle in the United States;
- U.S. citizens who wish to adopt internationally;
- Individuals who cannot immigrate to the United States for specific reasons and who wish to have those reasons waived;
- Members of the U.S. military and their families who wish to become U.S. citizens;

¹ The IO workforce includes two main components: International offices and 25 overseas Field Offices and Domestic Offices, as well as IO Headquarters in Washington, D.C. with satellite offices in Miami, Florida, and Anaheim, California. The three overseas District Offices are: Latin America, Canada, and the Caribbean; Asia/Pacific; and Europe, the Middle East, and Africa.



- Individuals who may qualify to enter the United States because they are recognized by U.S. law as being members of specific categories with a special need, such as widows or widowers of U.S. citizens;
- Individuals who request permission to enter the United States temporarily for urgent humanitarian reasons or reasons of significant public benefit;²
- LPRs who have traveled internationally and have lost their green cards; and
- LPRs who wish to abandon their permanent resident status in the United States.

Management of International Operations Cases

CAMINO is a person-centric case management system used to administer, track, and adjudicate applications filed with or processed by USCIS IO offices under IO jurisdiction with an international nexus. IO staff use CAMINO to manage the following application adjudication process: (1) Receipting and Acceptance Processing; (2) General Adjudication Procedures; (3) Security Screening Checks; (4) Interview; (5) Decision Case Action; and (6) Post-Adjudication.

1. Receipting and Acceptance Processing

When an IO office receives an application, IO staff conduct a preliminary review of the application to verify the following requirements: completed basic biographical information, jurisdiction, signature on the form, whether a correct fee has been paid (if applicable), and basic eligibility of the individual. USCIS rejects improperly filed applications, when applicable, with a written explanation as to why the application was rejected and any corrective action needed.

IO staff enter information about the applicant, petitioner, sponsor, and beneficiary from accepted applications into CAMINO. CAMINO then aggregates all previous cases associated with the individual within CAMINO and presents it to the IO staff in a single view. CAMINO provides a view of the individual's identity, immigration status, past applications adjudicated by IO since the implementation of CAMINO, and results of previous background identity and security checks. IO staff notifies the individual that USCIS received his or her application and is processing it by a CAMINO-generated receipt letter. This notice is saved in the case record in CAMINO.

CAMINO currently manages many types of application and petition forms, each with its own unique requirements and data elements.³ CAMINO is configured to collect certain data elements based on the specific type of application. Data elements may include: full name, alias(es),

² The Secretary of Homeland Security may "in his discretion parole into the United States temporarily [...] for urgent humanitarian reasons or significant public benefit any alien applying for admission to the United States." Immigration and Nationality Act § 212(d)(5), 8 U.S.C. § 1182(d)(5). *See also* 8 CFR § 212.5(b). USCIS, U.S. Immigration and Customs Enforcement (ICE), and U.S. Customs and Border Protection (CBP) share jurisdiction to adjudicate requests for parole, to include parole based on urgent humanitarian reasons or significant public benefit. More information is available at <http://www.ice.gov/doclib/foia/reports/parole-authority-moa-9-08.pdf>.

³ *See* Appendix A for a full list of applications processed by CAMINO.



physical and mailing address, phone numbers, e-mail address, current immigration status, citizenship, nationality, birth date, birth city, birth country, Social Security number (SSN), Alien Number (A-Number), passport number, and gender.

2. Adjudication Procedures

During the adjudication process, IO staff review all case-related information provided by the applicant and, if applicable, in the applicant's Alien File (A-File) to verify the identity and benefit eligibility of the applicant.⁴

Supporting Documentation

Supporting documentation is the initial evidence that USCIS requires as proof of identification and as justification of eligibility for a benefit. Examples of supporting documentation include copies of civil documents such as birth, marriage, or adoption certificates; divorce decrees; affidavits of financial support; or school records. Certain applications require applicants to provide credible evidence establishing a relationship between the petitioner and beneficiary.⁵

IO staff examine the application package to ensure all supporting documents are present. In situations in which evidence is missing or all required initial evidence is submitted but does not establish eligibility, USCIS may request that the applicant supply additional information through a Request of Evidence (RFE)⁶ or Notice of Intent to Deny (NOID)⁷ for continued processing.⁸ IO staff use CAMINO to generate and store most RFEs and NOIDs. If an applicant or petitioner does not respond to the RFE or NOID by the required date,⁹ USCIS may deny the application as abandoned or deny the application on the record.¹⁰

⁴ An A-File is a series of records maintained on an individual that document his or her history of interaction with USCIS, CBP, and ICE as prescribed by the Immigration and Nationality Act (INA) and other regulations regarding immigration benefits. *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (Nov. 21, 2013).

⁵ *See, e.g.,* Form I-130, *Petition for Alien Relative*; Form I-131, *Application for Travel Document*; Form I-360, *Petition for Amerasian, Widow(er), or Special Immigrant*; Form I-600, *Petition to Classify Orphan as an Immediate Relative*; Form I-601, *Application for Waiver of Grounds of Inadmissibility*; Form I-730, *Refugee/Asylee Relative Petition*, available at www.uscis.gov.

⁶ USCIS uses an RFE when an application lacks required documentation or the IO employee needs additional evidence to determine an applicant's eligibility for the benefit sought. The request will indicate what evidence or information is needed for USCIS to fully evaluate the application or petition under review.

⁷ A NOID is a formal statement from USCIS that it has determined that the applicant is ineligible for the immigrant benefit requested. The issuance of a NOID is required when derogatory information is uncovered during the course of the adjudication that is not known to the individual, according to 8 CFR § 103.2(b)(16). However, USCIS will grant the applicant an opportunity to overcome this determination and demonstrate that he or she is eligible.

⁸ *See* 8 CFR § 103.2(b)(8).

⁹ Generally, the standard maximum response time is 12 weeks (84 days). IO staff, in his or her discretion, may reduce the standard response time only after obtaining supervisory concurrence. This discretion is to be used on a case-by-case basis when warranted by circumstances as determined by the IO officer and the supervisor.

¹⁰ Individuals may submit a motion to reopen, which is a request for USCIS to review a decision. If the underlying application was denied due to abandonment (e.g., failure to respond timely to an RFE or a NOID), a motion to reopen



DNA Testing

In situations in which credible evidence is insufficient to prove a claimed biological relationship,¹¹ IO staff may suggest deoxyribonucleic acid (DNA) testing through an RFE.¹² USCIS has no statutory or regulatory authority to require DNA testing. Although USCIS may not require DNA testing, USCIS may suggest DNA testing, which may be completed at the option of the applicant to validate a claimed parent-child relationship in support of immigration benefits.¹³ Individuals who opt to submit DNA in response to a USCIS RFE are responsible for arranging the DNA test with a lab accredited by the American Association of Blood Banks (AABB).

Once testing is completed, AABB-accredited laboratories send all test results directly to the USCIS office that suggested the testing and to the petitioner that initiated the testing with the laboratory in the United States. The IO staff enter the following results information into CAMINO: (1) nature of the relationship being tested; (2) laboratory that performed the test; (3) date the test was requested; (4) date the DNA sample was taken; (5) date the DNA result was received; (6) result (confirmed or not confirmed); and (7) conclusiveness (probability of claimed parent-child relationship as expressed as a percentage) of the results. USCIS requires that the results must be 99.5% or higher to conclusively establish the parent-child relationship. USCIS only receives and retains data about DNA test results, limited to the information described above. USCIS does not receive, store, or share any other DNA information. USCIS neither requests nor collects the actual DNA. USCIS only uses the DNA results to verify claimed biological parent-child relationships.

DNA testing is voluntary; however, individuals who choose not to provide DNA samples may be unable to establish the qualifying relationship necessary to obtain the immigration benefit if

may be filed if it can be shown that the requested evidence was not material, the required initial evidence was submitted with the application, the applicant complied with USCIS' request for appearance or additional evidence during the allotted period, or the request for evidence or appearance was not sent to the address of record.

¹¹ USCIS verifies family relationships by examining documents, primarily civil records such as birth and marriage certificates and divorce and adoption decrees; in some cases USCIS may interview petitioners or intended beneficiaries. However, there may be instances when these verification measures are insufficient, such as when there is no documentary evidence available.

¹² See 8 CFR §§ 103.2(b)(2)(i), 204.2(d)(2)(v); see also Adjudicator's Field Manual (AFM), Chapter 21.2(d)(1)(B), available at www.uscis.gov.

¹³ An American Association of Blood Banks (AABB)-accredited laboratory uses a mouth swab to collect a DNA sample of an individual located in the United States. If an individual who needs to be tested is located overseas, the AABB-accredited laboratory sends a test kit to the USCIS overseas field office, or in the case in which USCIS is not present, to the U.S. Embassy or Consulate in an envelope sealed with security tape. A panel physician or other organization designated by the U.S. Embassy or USCIS office with jurisdiction over that individual's residence collects the DNA sample by mouth swab. When USCIS has an office overseas, USCIS serves as a witness overseeing the sample collection. When USCIS does not have an office overseas, the Department of State (DOS) serves as the witness overseeing the DNA sample collection. This oversight includes maintaining the chain of custody of the test kit and the collected DNA sample until the sample is mailed to the appropriate AABB-accredited lab chosen by the applicant or petitioner for parentage testing. USCIS personnel log in CAMINO and on the AABB-accredited lab's chain-of-custody forms the key steps taken to maintain proper chain-of-custody, including the receipt and secured storage of the test kit and mailing of the DNA sample back to the AABB-accredited lab for testing.



they are unable to present sufficient evidence to establish a requisite biological relationship in the absence of DNA results. The failure to provide DNA results in those circumstances may delay a final decision or result in denial of the benefit request.

A-File Review

IO staff may retrieve and review an applicant's A-File when adjudicating an application. IO staff may consolidate the application, supplemental documentation, and any other case information into the applicant's A-File. IO staff may also use the A-File to determine if the applicant has had prior involvement with USCIS or DHS Components. The A-File documents an individual's benefits and law enforcement transactions as he or she passes through the U.S. immigration and inspection process. This information may contain information relevant to establishing eligibility for the immigration benefit.

3. Security Screening Checks¹⁴

All individuals submitting applications to USCIS for immigration benefits may be subject to criminal and national security background checks to ensure eligibility for the requested benefit and to ensure that they do not pose a threat to public safety or the national security of the United States. USCIS conducts background and security checks before making a decision on the application.

IO staff performs background checks by querying a number of USCIS, DHS, and other U.S. Government systems.¹⁵ The background checks allow the IO staff to determine if there are criminal or security-related issues in the applicant's background that may affect his or her eligibility for immigration benefits. IO staff enters background check results into CAMINO. This information includes: source and date of the background check, whether the check returned any derogatory results, whether those results were resolved, and expiration date of the results. CAMINO does not communicate directly with any external background check systems. All background check results are either initiated through manual or electronic processes. Once received, IO staff manually records background check results (including source and date of the background check, whether the check returned any derogatory results, whether those results were resolved, and expiration date of the results) in CAMINO. A summary of the background checks may also be printed and stored in an A-File if required by standard operating procedures.

4. Interview

USCIS conducts interviews for certain applications as part of the benefit adjudication process. An applicant may be required to appear for an interview at an international office. IO staff use CAMINO to track the date and status of interview appointments and generate interview notices.

¹⁴ See DHS/USCIS/PIA-033 Immigration Benefits Background Check Systems (IBBCS), available at www.dhs.gov/privacy for more information about the USCIS security screening process.

¹⁵ See Appendix C for a list of DHS, USCIS, and U.S. Government systems used to conduct background checks as well as a full description of each background check.



Each interview appointment is linked to the applicant's record. CAMINO stores the following information about the applicant's interview: date, time, location, status, notice sent date, and access secured (i.e., whether the applicant has been granted access to the Embassy or Consulate, if required). For certain applications, USCIS may also store an interview worksheet in CAMINO. IO staff mails the Interview Notice to the applicant and, if applicable, his or her representative. Interview information is also added to the A-File if required by case adjudication standard operating procedures.

5. Case Decision

After all the above steps, IO staff makes a determination on the application. IO staff may grant, deny, or revoke an immigration benefit. IO staff may also allow the applicant or petitioner to withdraw their request for the benefit. In certain circumstances, an application for an immigration benefit may also be administratively closed. Case decision actions are tracked and recorded in CAMINO. During the decision-making process, the following may occur:

- USCIS approves the application and issues an approval letter;
- USCIS issues a RFE and NOID to request additional information needed to adjudicate the application;
- USCIS denies the application and issues a denial letter detailing the decision and the reason for the decision is issued;
- USCIS revokes the benefit and issues a revocation letter detailing the decision is issued;¹⁶
- USCIS issues a notice to acknowledge the withdrawal of the benefit request; or
- USCIS administratively closes the application and issues a letter detailing why the letter issued.

For most applications, CAMINO generates and maintains notices of decisions to applicants for future reference. USCIS consolidates notices sent to the applicant and his or her representative into the A-File. Final decisions are also manually recorded in primary USCIS case management systems including Computer Linked Application Information Management System (CLAIMS) 3 and CLAIMS 4.¹⁷

¹⁶ See 8 CFR § 205.2.

¹⁷ See DHS/USCIS/PIA-016 Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3); DHS/USCIS/PIA-015 USCIS Computer Linked Application Information Management System (CLAIMS 4), available at www.dhs.gov/privacy.



6. *Post-Decision Reporting*

USCIS uses the information contained in CAMINO to generate a number of statistical reports to measure and evaluate workload for proper resource allocation. CAMINO interfaces with Standard Management Analysis and Reporting Tool (SMART) to create customizable reports for a variety of purposes.¹⁸ USCIS generates reports to identify cases pending at all IO offices to measure productivity trends and average processing times. USCIS also generates granular level reports to identify types, number, and status of cases located in a particular office or assigned to a particular IO staff member, which allows supervisors to identify the oldest cases in queue for processing.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Section 103 of the Immigration and Nationality Act (INA) provides the legal authority for this system.¹⁹

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The following SORNs cover the collection, maintenance, and use of the information contained in CAMINO:

- Alien File, Index, and National File Tracking System²⁰ covers the collection, use, and maintenance of applications and supplemental evidence,
- Background Check Service²¹ covers background checks and its results,
- Inter-Country Adoptions Security²² covers the collection and use of adoption applications, decisional data, and associated fees for adjudication,
- Benefits Information System²³ covers the collection and use of immigrant and nonimmigrant benefit applications, decisional data, and associated fees for adjudication for adjudication, and

¹⁸ See DHS/USCIS/PIA-050 SMART, available at www.dhs.gov/privacy.

¹⁹ 8 U.S.C. § 1103.

²⁰ DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (Nov. 21, 2013).

²¹ DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007).

²² DHS/USCIS-005 Inter-Country Adoptions Security, 72 FR 31086 (June 5, 2007).

²³ DHS/USCIS-007 Benefits Information System, 73 FR 56596 (Sept. 29, 2008).



- Asylum Information and Pre-Screening²⁴ covers the collection and use of affirmative asylum applications, applications filed with USCIS for suspension of deportation, special rule cancellation of removal pursuant to the Nicaraguan Adjustment and Central American Relief Act,²⁵ credible fear screening cases,²⁶ and reasonable fear screening cases.²⁷

1.3 Has a system security plan been completed for the information system(s) supporting the project?

CAMINO is covered as a minor system under the Digital Innovation and Development – Information Technology (DID-IT) accreditation boundary. DID-IT completed the security assessment and authorization documentation in August 2013, and was accepted into the Ongoing Authorization program. Ongoing Authorization requires DID-IT, including CAMINO, to be reviewed on a monthly basis and maintain its security posture to maintain its ATO.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

NARA approved the CAMINO retention schedule [N1-566-12-06] on April 17, 2013. CAMINO retains records 25 years from the date of the last completed action. Supplemental evidence submitted along with the application or provided through an RFE is stored in the A-File [N1-566-08-11]. A-File records are permanent, whether hard copy or electronic. DHS transfers A-Files to the custody of NARA 100 years after the individual's date of birth.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

USCIS collects most of the information contained in CAMINO directly from the applicant through completed immigration forms, which are subject to PRA requirements. A list of the immigration forms processed in CAMINO, along with the OMB Control Numbers is available in Appendix A.

²⁴ DHS/USCIS-010 Asylum Information and Pre-Screening, 75 FR 409 (Jan. 5, 2010).

²⁵ See Nicaraguan Adjustment and Central American Relief Act, Pub. L. No. 105-100, § 203, 111 Stat. 2193, 2196-200 (1997).

²⁶ See 8 U.S.C. § 1225(b)(1)(B).

²⁷ See 8 CFR § 208.31.



Section 2.0 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.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

CAMINO maintains information from applications for immigration benefits adjudicated or processed by USCIS IO offices located both overseas and domestically.²⁸ The information extracted from these forms varies and not all forms collect the same information. CAMINO may retain the following data elements:

Names: first name, last name, middle name, and any aliases of applicants, petitioners, sponsors, beneficiaries, and in cases of intercountry adoptions, household members. USCIS also collects names from form sponsors, preparers, attorneys, and designated representatives.

Immigration Status: e.g., LPR, U.S. citizen, asylee, refugee, or parolee, relating to applicants, petitioners, beneficiaries, sponsors, and, in the case of intercountry adoptions, household members.

Physical and Mailing Address: applicants, beneficiaries, petitioners, sponsors, attorneys, representatives, and, in the case of intercountry adoptions, household members and adoption service providers.

Telephone Numbers: applicants, beneficiaries, petitioners, sponsors, household members, consular posts, sponsors, attorneys, representatives, and, in the case of intercountry adoptions, household members and adoption service providers.

E-mail Addresses: applicants, petitioners, sponsors, beneficiaries, household members, attorneys, representatives, and in the case of intercountry adoptions, household members and adoption service providers.

Birth Dates: applicants, beneficiaries, petitioners, sponsors, spouses, parents, siblings, children/stepchildren/adopted children, and in the case of intercountry adoptions, household members.

A-Number: applicants, beneficiaries, petitioners, sponsors, and in the case of intercountry adoptions, household members.

SSN: applicants, beneficiaries, petitioners, sponsors, and in the case of intercountry adoptions, household members.

Citizenship/Nationality: applicants and beneficiaries.

²⁸ See Appendix A for a complete list of these forms.



Gender: applicant, petitioner, sponsor, beneficiary, and in the case of intercountry adoptions, household members.

DNA Test Results: DNA test results from an AABB-accredited laboratory to verify a claimed biological parent-child relationship (i.e., the nature of the relationship being tested, laboratory name, date the test was requested, date the DNA sample was taken, date the DNA result was received, the result, and the conclusiveness of the results).²⁹

Results of Background Identity and Security Checks: date of the background check, whether the check returned any derogatory results, whether those results were resolved, and expiration date of the results. IO staff manually enters background check results in CAMINO. Certain background check results are uploaded into CAMINO in a semi-automated batch process.

Final Decision: includes a notice to the applicant and the representative on record.

2.2 What are the sources of the information and how is the information collected for the project?

Most of the information in CAMINO is derived from the data provided by the applicant on the completed immigration form and from documentation in support of his or her application. IO staff manually enter information submitted on the USCIS application into CAMINO. DNA and most background check results are also manually entered into CAMINO. Certain background check results are uploaded into CAMINO in a semi-automated batch process. Please see the Appendices for a full list of immigration forms and background checks tracked in CAMINO.

²⁹ In Overseas Processing cases, the overseas officer issues an RFE suggesting DNA testing to the applicant/petitioner when the officer is unable to either adjudicate a case or issue a travel document based on the documentary evidence available. If the applicant/petitioner opts to submit DNA, he or she arranges the DNA testing through an AABB-accredited facility, and has any sampling of those located in the United States completed at the AABB-accredited facility. USCIS only collects the DNA results from the lab. USCIS neither requests nor collects the actual DNA. In an immigration benefit adjudication that requires verifying a parent-child relationship, the applicant/petitioner must provide evidence of the claimed relationship. The burden is on the applicant/petitioner to establish that he or she is eligible for the benefit sought. Generally, birth certificates are treated as the best available primary evidence of a parent-child relationship. When primary evidence is unavailable, the applicant/petitioner must demonstrate that it is not available and submit secondary evidence such as a baptismal certificate, church records, or school records. If the applicant/petitioner demonstrates that such secondary evidence is unavailable, two or more affidavits from individuals with reason to know about the claimed relationship may be substituted. However, the unavailability of a birth certificate creates a presumption of ineligibility for the benefit, and any alternative evidence submitted must be evaluated for its authenticity and credibility. IO staff should request and evaluate all documentary evidence before suggesting DNA. Officers must exhaust all other possible methods of confirming a relationship before suggesting a DNA test; DNA testing should generally be a last resort.



2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4 Discuss how accuracy of the data is ensured.

USCIS collects information primarily from the individual applicant or his or her representative. CAMINO helps validate data entry through program coding to mitigate or prevent inconsistencies in applicant data and in decision processing entries (e.g., the system rejects 00/00/00 birthdates). Data entry personnel are provided with the opportunity to review and edit information prior to and after their submission. IO staff verify the accuracy by comparing information provided by the individual with information contained in the individual's A-File, on his or her DNA results, and from federal law enforcement systems.³⁰ USCIS also verifies data accuracy with the applicant during the applicant interview. IO staff can correct and edit inaccuracies at any stage of the process.

Furthermore, IO Headquarters (HQ) generates standard and custom reports on a regular basis to identify incorrectly entered cases. HQ uses the CAMINO custom query functionality to search for specific types of errors, for example cases in which an "Arrived at IO date" has not been entered. IO HQ remedies trends of incorrect data entry by conducting specialized training.

With respect to oversight of DNA collection, USCIS follows proper chain of custody procedures in alignment with AABB-accredited laboratory procedures.³¹ The DNA laboratory analyzing the DNA samples sends a copy of the results, but not the actual DNA, directly to USCIS identifying the degree of probability that a claimed relationship exists.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of inaccurate data due to manual data entry from multiple security screening systems.

Mitigation: This risk is only partially mitigated due to the amount of data that USCIS manually enters from security screening systems. However, USCIS is working to automate this process and remove the opportunity for human error. In addition, ensures data accuracy through program coding to mitigate or prevent inconsistencies in applicant data and in decision processing

³⁰ USCIS uses multiple federal law enforcement systems to conduct security checks for all cases involving an application for an immigration service or benefit. This is done to both enhance national security and ensure the integrity of the immigration process. Please see Appendix C to view a list of background checks tracked in CAMINO.

³¹ See *supra* text accompanying note 13.



entries, employee training, and finally during the applicant interview where applicants are able to confirm data accuracy.

Privacy Risk: There is a risk of overcollection of information for making a benefit determination.

Mitigation: The USCIS Privacy Office reviews each immigration form during the development process to ensure that only the minimum amount of information is collected to determine benefit eligibility. Furthermore, all data elements collected are negotiated with and approved by OMB during PRA collection review.

In an immigration benefit adjudication that requires verifying a parent-child relationship, the applicant must provide evidence of the claimed relationship. The burden is on the applicant to establish that he or she is eligible for the benefit sought. In Overseas Processing cases, IO staff issue a RFE suggesting, not requiring, DNA testing to the applicant when he or she is unable to either adjudicate a case or issue a travel document based on the documentary evidence available. If the applicant opts to submit DNA, he or she arranges the DNA testing through an AABB-accredited facility. USCIS receives only the DNA results from the lab. The actual DNA is not requested or collected by USCIS. See footnote 13 for information on USCIS witnessing of panel physicians in certain circumstances when DNA is collected abroad.

USCIS designed CAMINO specifically to collect and store only the information that is necessary to adjudicate the applications processed by IO under its jurisdiction with an international nexus. USCIS requires the information collected and stored in CAMINO to establish the identity of the applicant, petitioner, or beneficiary, and to process the benefit request to determine benefit eligibility.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

USCIS uses CAMINO to support and manage the administration and adjudication of all applications received and adjudicated by IO under IO jurisdiction with an international nexus. Specific uses of CAMINO and the information it contains include:

- Identify missing information and to make requests for additional information;
- Provide a repository of data to assist with future immigration benefit applications and requests;
- Schedule interview and biometrics appointments;



- Maintain security screening check results to determine suitability for immigration benefits using criminal, immigration, or terrorism-related history;
- Generate and issue decision notices;
- Manage workflow; and
- Generate reports.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that authorized users could use the data for purposes inconsistent with the original collection.

Mitigation: Access to CAMINO is limited to USCIS employees. To ensure the information is used consistently with the purposes of the original collection, USCIS monitors user logs to ensure users are only accessing information related to their job functions. Prior to accessing CAMINO, each user must sign a user access agreement that outlines the appropriate rules of behavior tailored to CAMINO. USCIS implements disciplinary rules to ensure the appropriate use of the system. USCIS reminds employees accessing the system that the system may be monitored for improper use and illicit activity, and the penalties for non-compliance, through a warning banner that reiterates the appropriate uses of the system. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. This acts as a deterrent to unauthorized activity.

Privacy Risk: There is a risk that unauthorized users may gain access to CAMINO.

Mitigation: All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards such as restricting access to authorized personnel who have a need-to-know. CAMINO is a web-based application that is only available through the DHS USCIS network.³² Access to CAMINO is granted to only a limited number of users for

³² USCIS IO offices located both overseas and domestically access and log into CAMINO through the DHS OneNet,



determining benefit eligibility. CAMINO users must have access to the USCIS network and have USCIS credentials. Users must authenticate their credentials to gain access to the system. USCIS also employs auditing capabilities that log user activity.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Individuals are provided general notice through the publication of this PIA and the Alien File, Index, and National File Tracking System,³³ Inter-Country Adoptions Security,³⁴ Background Check Service,³⁵ Benefit Information System,³⁶ and Asylum Information and Pre-Screening³⁷ SORNs.

Additionally, the instructions associated with each immigration form contain a Privacy Act Statement. Each Privacy Act Statement provides notice to individuals about the agency's authority to collect information, the purposes of data collection, routine uses of the information, and the consequences of declining to provide the requested information to USCIS.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The submission of a benefit request is voluntary. To grant the requested benefit, applicants must provide certain biographic and biometric information that may include submission of fingerprints, photographs, and signatures, in addition to other information requested in an application. This information is critical in making an informed adjudication decision to grant or deny an immigration benefit. Failure to provide the requested information prohibits USCIS from processing and properly adjudicating the application and thus precludes the applicant from receiving the benefit.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may be unaware of the purposes for which

which is a secured local area network.

³³ DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (Nov. 21, 2013).

³⁴ DHS/USCIS-005 Inter-Country Adoptions Security, 72 FR 31086 (June 5, 2007).

³⁵ DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007).

³⁶ DHS/USCIS-007 Benefits Information System, 73 FR 56596 (Sept. 29, 2008).

³⁷ DHS/USCIS-010 Asylum Information and Pre-Screening, 75 FR 409 (Jan. 5, 2010).



their information is used.

Mitigation: All individuals (i.e., petitioner, beneficiary, applicant, sponsor) who submit an application for immigration benefits are made aware that the information they provide is collected for determining eligibility for immigration benefits. Each immigration form contains a Privacy Act Statement describing the legal authority to collect information, the purpose for the collection, routine uses of the collected information, and the right to decline to provide information. The Privacy Act Statement also advises applicants that the information provided may be shared with other federal, state, local, and foreign law enforcement and regulatory agencies during the course of the investigation. All USCIS Privacy Act Statements are approved by the USCIS Privacy Office.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

Under the approved retention schedule for CAMINO [N1-566-12-06], the system retains records 25 years from the date of the last completed action. This retention schedule allows IO to address any follow-up inquiries or requests related to the application, including inquiries related to security matters. Supplemental evidence submitted along with the application or provided through an RFE is stored in the A-File [N1-566-08-11]. A-File records are permanent, whether hard copy or electronic. DHS transfers A-Files to the custody of NARA 100 years after the individual's date of birth.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that CAMINO may retain information longer than is necessary to perform relevant immigration functions.

Mitigation: Although there is always risk inherent with retaining data for any length of time, CAMINO data retention periods are consistent with the concept of retaining data to maintain a complete and accurate history of an individual's immigration interaction with USCIS for future benefit requests.



Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

USCIS manually shares information from CAMINO with other federal agencies for the purpose of processing applications or petitions for benefits under INA, as previously described in the Overview section of this PIA during the third step, “Security Screening Checks,” of the management of international operations cases.³⁸ These other federal agencies include the Department of Defense (DOD), the Department of Justice (DOJ), the Department of State (DOS), and the National Counterterrorism Center (NCTC). These checks are conducted manually or electronically, and a record of those checks and their results (including source and date of the background check, whether the check returned any derogatory results, whether those results were resolved, and expiration date of the results) are manually entered into CAMINO. There is no electronic communication between the external systems and CAMINO.

Please see Appendix C for a full list and analysis of all external sharing arrangements.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

USCIS shares CAMINO information under the routine uses outlined in the applicable SORNs:

DOD

USCIS shares data with DOD under routine use P of the A-File SORN, and routine use J of the Benefits Information System SORN, which permit USCIS to share information with other government agencies during the processing of a matter under DHS’s jurisdiction or during a proceeding within the purview of the immigration and nationality laws, when DHS deems that disclosure is necessary to carry out its functions and statutory mandates.³⁹ Background Check System routine use H also permits DHS to share information with government intelligence or counterterrorism agencies when DHS becomes aware of an indication of a threat or potential threat to national or international security, or when used to conduct national intelligence and security

³⁸ Please see Appendix C for a full list of external identity and background checks tracked in CAMINO.

³⁹ See DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (Nov. 21, 2013); DHS/USCIS-007 Benefits Information System, 73 FR 56596 (Sept. 29, 2008).



investigations or assist in anti-terrorism efforts. USCIS conducts this vetting to determine if information exists that might render the individual ineligible for the requested benefit or request and stores the results in CAMINO.

DOS

USCIS shares data with DOS under routine use O of the A-File SORN, routine use B of the Intercountry Adoptions SORN, and routine use I of the Benefits Information System SORN, which permit DHS to share information with DOS in the processing of applications for benefits under the INA, and all other immigration and nationality laws including treaties and reciprocal agreements.⁴⁰ Asylum Information Pre-Screening SORN routine use I also permits DHS to share information with other government agencies during the processing of a matter or during a proceeding within the purview of the immigration and nationality laws, when DHS deems that disclosure is necessary to carry out its functions and statutory mandates.⁴¹ USCIS conducts this vetting to determine if information exists that might render the individual ineligible for the requested benefit or request and stores the results in CAMINO.

DOJ FBI

USCIS shares data with FBI under the Background Check Service SORN.⁴² Background Check System routine use H permits DHS to share information with government intelligence or counterterrorism agencies when DHS becomes aware of an indication of a threat or potential threat to national or international security, or when used to conduct national intelligence and security investigations or assist in anti-terrorism efforts. USCIS conducts this vetting to determine if information exists that might render the individual ineligible for the requested benefit or request and stores the results in CAMINO.

NCTC

USCIS shares CAMINO data under the Asylum Information and Pre-Screening and A-File SORNs. Asylum Information and Pre-Screening routine use H permits DHS to share information with government intelligence or counterterrorism agencies when DHS becomes aware of an indication of a threat or potential threat to national or international security, or when used to conduct national intelligence and security investigations or assist in anti-terrorism efforts. DHS also shares CAMINO data under routine use P of the A-File SORN and routine use I of the Asylum Information Pre-Screening SORN, which permit DHS to share information with other government agencies during the processing of a matter under DHS's jurisdiction or during a proceeding within

⁴⁰ See DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (Nov. 21, 2013); DHS/USCIS-005 Inter-Country Adoptions Security, 72 FR 31086 (June 5, 2007); DHS/USCIS-007 Benefits Information System, 73 FR 56596 (Sept. 29, 2008).

⁴¹ See DHS/USCIS-010 Asylum Information and Pre-Screening, 75 FR 409 (Jan. 5, 2010).

⁴² See DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007).



the purview of the immigration and nationality laws, when DHS deems that disclosure is necessary to carry out its functions and statutory mandates. USCIS conducts this vetting to determine if information exists that might render the individual ineligible for the requested benefit or request and stores the results in CAMINO.

6.3 Does the project place limitations on re-dissemination?

DHS or USCIS enters into Memoranda of Understanding/Agreement (MOU/A) with external organizations prior to the systematic sharing of information. When sharing information with parties outside of DHS, the same specifications related to security and safeguarding of privacy-sensitive information that are in place for USCIS and DHS are applied to the outside entity. The agreements between DHS and external entities (e.g., DOD, DOS, DOJ, and NCTC) fully outline responsibilities of the parties, security standards, and limits of use of the information, including re-dissemination, prior to information sharing. Access to records is governed by need-to-know criteria that demand the receiving entity demonstrate the mission-related need for the data before access is granted. In the terms of a negotiated agreement or the language of an authorization providing information to an external agency, USCIS includes justification for collecting the data, and an acknowledgement that the receiving agency will not share the information without USCIS or DOS's permission, as applicable.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

USCIS IO keeps an electronic record of all CAMINO records sent to non-DHS partners to screen for benefit eligibility. Furthermore, USCIS updates individual CAMINO case records to reflect that a specific check has been completed.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that data shared by USCIS with external partners will be used beyond the original purpose of collection (immigration benefits).

Mitigation: USCIS is careful to share data with external agencies that have a need to know, and put the information to a use that is compatible with USCIS SORNs. USCIS documents these safeguards in MOU/A with the external partners. USCIS manually shares information from CAMINO with other federal agencies and there is no electronic communication between the external system and CAMINO. All prospective information handlers must be authorized to access the information. This mitigates the risk of unauthorized disclosure by requiring a trained employee with access to the information to review the information before sharing the information with an external agency.

Privacy Risk: There is a risk that data shared by USCIS will be retained longer than necessary by external partners.



Mitigation: USCIS enters into MOU/A with all recipient agencies that detail specific retention requirements for all security vetting initiatives. Specific MOU/A provisions are discussed in the Appendices to this PIA. These MOU/As discuss the parties' respective responsibilities for safeguarding, retaining, and using the information. Additionally, receiving agency personnel have been trained on proper use of sensitive information and understand that they may only provide the information to those who have a need to know and with USCIS' authorization.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

An individual may gain access to his or her USCIS records by filing a Privacy Act request. If an individual would like to file a Privacy Act request to view his or her USCIS record, he or she may mail the request to the following address:

National Records Center
Freedom of Information Act (FOIA)/Privacy Act Program
P. O. Box 648010
Lee's Summit, MO 64064-8010

The information requested may be exempt from disclosure under the Privacy Act because information contained within CAMINO may contain law enforcement sensitive information, the release of which could possibly compromise ongoing criminal investigations. Further information about Privacy Act and FOIA requests for USCIS records is available at <http://www.uscis.gov>.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals should submit requests to contest or amend information contained in CAMINO as discussed in Section 7.1. The requestor should clearly and concisely state the information being contested, the reason for contesting or amending it, and the proposed amendment. The requestor should also clearly mark the envelope, "Privacy Act Amendment Request." The record must be identified in the same manner as described for making a request for access.



7.3 How does the project notify individuals about the procedures for correcting their information?

USCIS notifies individuals of the procedures for correcting their information in the privacy compliance documentation covering CAMINO, Privacy Act Statements, and through USCIS personnel who interact with them. Specifically, the SORNs set forth in Section 1.2 provide individuals with guidance regarding the procedures for correcting information. This PIA also provides similar notice. The Privacy Act Statements, including notice of an individual's right to correct information, are also contained on the instructions to immigration forms published by USCIS. USCIS notifies individuals during their interview about the procedures for correcting application information as maintained in CAMINO.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: The Privacy Act of 1974 permits a federal agency to exempt a system of records from some of the Act's requirements, such as access and redress. There is a risk that the right to redress may be limited by Privacy Act exemptions or limited avenues for seeking redress.

Mitigation: USCIS gives individuals numerous opportunities during and after the completion of the application process to correct information they have provided and to respond to information received from other sources. Individuals may avail themselves of the redress and appeal process as stated in the DHS Privacy Act regulations, 6 CFR § 5.21. In addition, USCIS provides all applicants or petitioners an opportunity to refute benefit determinations during the in-person interview phase described in the Overview.

Privacy Risk: There is a risk that individuals will not have redress from external partner agencies with which USCIS shares CAMINO information.

Mitigation: USCIS has mitigated this risk to the best extent possible. USCIS sends to and obtains information from external agencies, as described in the Appendices to this PIA. These external agencies are fully responsible for any data that they provide to USCIS. They are responsible for maintaining accurate records obtained from USCIS. The external agencies provide procedures for access and redress in accordance with the FOIA and Privacy Act. Individuals may seek more information on access, redress, or correction by reviewing the PIA for the individual system. In addition, Appendix B lists the applicable SORN, which identifies the redress procedures for the external system.



Section 8.0 Auditing and Accountability

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

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

CAMINO is designed with strict auditing capabilities that log the activity of each user to reduce the possibility of misuse and inappropriate dissemination of information. In accordance with DHS security guidelines, CAMINO uses auditing capabilities that logs user activity. USCIS tracks all user actions via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

USCIS employees and contractors are required to complete annual Privacy and Computer Security Awareness Training to ensure their understanding of proper handling and securing of PII. Privacy training addresses appropriate privacy concerns, including Privacy Act obligations (e.g., SORNs, Privacy Act Statements). The Computer Security Awareness Training examines appropriate technical, physical, and administrative control measures. Leadership at each USCIS office is responsible for ensuring that all federal employees and contractors receive the required annual Computer Security Awareness Training and Privacy training.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

In the course of its standard onboarding procedures, new employees are assigned a role in CAMINO appropriate to the employee's position and need-to-know. Once the employee is assigned to an overseas office or to a headquarters branch, the employee's supervisor is responsible for validating the employee's continued access to CAMINO.

If USCIS users outside of IO wish to have access to CAMINO, he or she must secure sponsorship from an IO employee who can verify the party's need-to-know. IO documents the identity of the sponsor and the reason for access, allowing IO to re-verify access as needed.

CAMINO links a user's profile to his or her Windows network credentials and uses Active Directory (AD) to control which users may access the system and to ensure users are assigned permissions appropriate to their role.



8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

USCIS has a formal review and approval process in place for new sharing agreements. Any new use of information and/or new access requests for the system must go through the USCIS change control process and must be approved by the proper authorities of this process, such as the USCIS Privacy Officer, Chief of Information Security Officer, Office of Chief Counsel, and the respective Program Office.

Responsible Officials

Donald Hawkins
Privacy Officer
United States Citizenship and Immigration Services

Approval Signature

Original signed copy on file with the DHS Privacy Office.

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security



APPENDIX A

USCIS Immigration Forms and Associated OMB Control Numbers

Form Number	Title	OMB Control Number
G-146	Voluntary Departure Form	1115-0075
I-130	Immigrant Petition for Alien Relative	1615-0012
I-131	Application for Travel Document	1615-0013
I-131A	Application for Travel Document (Carrier Documentation)	1615-0135
I-134	Affidavit of Support	1615-0014
I-193	Application for Waiver of Passport and/or Visa	1651-0107
I-212	Application for Permission to Reapply for Admission into the United States After Deportation or Removal	1615-0018
I-290B	Notice of Appeal to the Administrative Appeals Office	1615-0095
I-360	Petition for Amerasian, Widow(er), or Special Immigrant	1615-0020
I-407	Abandonment of Lawful Permanent Residence Status	In Progress
I-590	Registration for Classification as Refugee	1615-0068
I-600	Petition to Classify Orphan as an Immediate Relative	1615-0028
I-600A	Application for Advance Processing of Orphan Petition	1615-0028
I-601	Application for Waiver of Ground of Excludability	1615-0029
I-602	Application By Refugee For Waiver of Grounds of Excludability	1615-0069
I-730	Refugee/Asylee Relative Petition	1615-0037
N-400	Application for Naturalization	1615-0052



N-600K

Application for Citizenship and Issuance of
Certificate under Section 322

1615-0057



APPENDIX C

List of Systems researched during the Background, Identity, and Status Check Process and Tracked in CAMINO

U.S. Citizenship and Immigration Services (USCIS) Systems

Central Index System (CIS)⁴³ contains information on the status of more than 57 million applicants/petitioners seeking immigration benefits including: LPRs, naturalized citizens, U.S. border crossers, aliens who illegally entered the United States, aliens who have been issued employment authorization documents, individuals who petitioned for benefits on behalf of family members, and other individuals subject to the provisions of the INA. USCIS uses this information to verify the current immigration status of individuals.

There is no electronic communication between CAMINO and CIS. USCIS conducts manual checks in CIS, and the record of those checks and their results are manually entered into CAMINO.

Computer Link Application Information Management System (CLAIMS) 3⁴⁴ and CLAIMS 4⁴⁵ process and manage applications for immigration-related benefits. USCIS uses CLAIMS 3 and CLAIMS 4 to review past and current immigration benefit filings and to obtain case status information.

USCIS manually conducts CLAIMS 3 and CLAIMS 4 checks, and the record of those checks and their results may be manually entered into CAMINO. There is no electronic communication between CAMINO and CLAIMS 3 or CLAIMS 4.

Customer Profile Management System (CPMS) is a centralized repository of USCIS biometrics data including the photo, fingerprint, and signature of applications. CPMS also supports the electronic transmission of data from USCIS to the FBI for conducting fingerprint biometric background checks in the FBI's Next Generation Identification (NGI) system⁴⁶ and stores the results of those checks, including all biographical and response data, including FBI criminal history (rap sheet) and civil applicant responses. USCIS uses the information for reference in the adjudication process.

CPMS generates reports containing FBI fingerprint results in a spreadsheet format, and that spreadsheet is then uploaded into CAMINO by IO HQ to record the FBI fingerprint checks and associated results for applicants in their individual case records in CAMINO. USCIS manually

⁴³ See DHS/USCIS/PIA-009 Central Index System PIA, available at www.dhs.gov/privacy.

⁴⁴ See DHS/USCIS/PIA-016 Benefits Processing of Applicants other than Petitions for Naturalization, Refugee, Status, and Asylum (CLAIMS 3) PIA, available at www.dhs.gov/privacy.

⁴⁵ See DHS/USCIS/PIA Computer Linked Application Information Management System (CLAIMS 4) PIA, available at www.dhs.gov/privacy.

⁴⁶ See FBI-009 Fingerprint Identification Records System (FIRS), 64 FR 52347 (Sept. 28, 1999).



conducts checks of CPMS checks, and manually enters the record of those checks and their results into CAMINO. There is no electronic communication between CPMS and CAMINO.

Other Department of Homeland Security (DHS) Component Systems

Customs and Border Protection (CBP)

TECS⁴⁷ is an automated enforcement and inspection lookout system that combines information from multiple agencies, databases, and system interfaces. Data in TECS covers Known and Suspected Terrorists (KST), other national security risks, public safety issues, warrants, travel information, and other law enforcement concerns. Evidence of criminality may include the existence of an FBI number, rap sheet, want/warrant, or a DHS Automated Biometric Identification System (IDENT),⁴⁸ TECS, or other law enforcement record.

IO staff manually conducts TECS checks, and manually enters the results into CAMINO. There is no electronic communication between TECS and CAMINO.

Automated Targeting System - Passenger (ATS-P)⁴⁹ is an intranet-based enforcement and decision support tool that is the cornerstone for all CBP targeting efforts. CBP uses ATS to improve the collection, use, analysis, and dissemination of information gathered for the primary purpose of targeting, identifying, and preventing potential terrorists and terrorist weapons from entering the United States. ATS-P is one of the five modules within ATS.

ATS-P is the module used at all U.S. airports and seaports receiving international flights and voyages to evaluate passengers and crewmembers prior to arrival or departure. ATS-P's screening relies upon the following databases: Advanced Passenger Information System (APIS),⁵⁰ Non Immigrant Information System (NIIS),⁵¹ Electronic System for Travel Authorization (ESTA),⁵² Border Crossing Information (BCI),⁵³ Suspect and Violator Indices (SAVI),⁵⁴ the Department of State visa databases, the Passenger Name Record information from the airlines, TECS crossing data, TECS seizure and enforcement data, information from the

⁴⁷ See DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing PIA, available at www.dhs.gov/privacy.

⁴⁸ See DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), available at www.dhs.gov/privacy. See also DHS/NPPD-004 IDENT, 72 FR 31080 (June 5, 2007).

⁴⁹ See DHS/CBP/PIA-006(b) Automated Targeting System (ATS), available at www.dhs.gov/privacy.

⁵⁰ See DHS/CBP/PIA-001 Advance Passenger Information System (APIS), available at www.dhs.gov/privacy. See also DHS/CBP-005 Advance Passenger Information System (APIS), 80 FR 13407 (Mar. 13, 2015).

⁵¹ See DHS/CBP-016 Nonimmigrant Information System, 80 FR 13398 (Mar. 13, 2015).

⁵² See DHS/CBP/PIA-007 Electronic System for Travel Authorization, available at www.dhs.gov/privacy. See also DHS/CBP-009 Electronic System for Travel Authorization (ESTA), 79 FR 65414 (Nov. 3, 2014).

⁵³ See DHS/CBP-007 Border Crossing Information (BCI), 80 FR 26937 (May 11, 2015).

⁵⁴ See DHS/CBP/PIA-006(b) Automated Targeting System (ATS), available at www.dhs.gov/privacy.



consolidated and integrated terrorist watch list maintained by the Terrorist Screening Center,⁵⁵ and DOS Consular Consolidated Database.⁵⁶

USCIS uses ATS-P to vet non-immigrant and immigrant visa applications. USCIS manually conducts checks of ATS-P, and manually records those checks and their results in CAMINO. There is no electronic communication between ATS-P and CAMINO.

Arrival and Departure Information System (ADIS)⁵⁷ collects information about non-citizens who travel to the United States. This includes arrival and departure border crossings, and immigration status updates for each traveler. ADIS receives information from multiple systems, some of which are from government organizations external to CBP, and matches events to a unique person to create a complete record of events during their U.S. visits. ADIS matches departures with arrivals to ascertain compliance, stores travel and status adjustment records, and provides a range of ad hoc queries and reporting capabilities. ADIS incorporates additional data elements and transactions associated with IDENT and other immigration systems to maintain complete traveler histories. ADIS maintains travel histories on over 200 million alien travelers.

USCIS uses ADIS information to verify an applicant's arrival to or departure from the United States as part of the determination of immigration benefits eligibility. USCIS manually conducts ADIS checks and records those checks and their results in CAMINO. There is no electronic communication between the ADIS system and CAMINO.

Immigration and Customs Enforcement (ICE)

ENFORCE Alien Removal Module (EARM)⁵⁸ tracks the status of alien removal proceedings from the United States. EARM provides personal identifiers, photographs, and details of removal case proceedings to aid ICE Detention and Removal Operations in carrying out the removal of aliens from the United States.

USCIS uses EARM to research an individual's immigration history to determine if an individual is eligible for an immigration benefit for which he or she has applied. USCIS manually conducts EARM checks and records those checks and their results in CAMINO. There is no electronic communication between CAMINO and EARM.

⁵⁵ See DHS/ALL/PIA-027(b) Watchlist Service (WLS) Update, available at www.dhs.gov/privacy.

⁵⁶ See Consular Consolidated Database (CCD) PIA, available at <http://www.state.gov/m/a/ips/c24223.htm>.

⁵⁷ See DHS/CBP/PIA-24 Arrival and Departure System (ADIS), available at www.dhs.gov/privacy.

⁵⁸ See DHS/ICE/PIA-015 Enforcement Integrated Database (EID); DHS/ICE/PIA-015(a) Enforcement Integrated Database (EID); DHS/ICE/PIA-015(b) Enforcement Integrated Database (EID); DHS/ICE/PIA-015(c) Enforcement Integrated Database (EID) ENFORCE Alien Removal Module Update; DHS/ICE/PIA-015(d) Enforcement Integrated Database (EID) ENFORCE Alien Removal Module Update, available at www.dhs.gov/privacy.



Office of Biometric Identity Management (OBIM, formerly US-VISIT)

Automated Biometric Identification System (IDENT)⁵⁹ The OBIM IDENT information technology system includes biometric information related to the travel history of non-U.S. citizens and biometric watchlist (KST) information. USCIS uses this system to confirm identity, determine previous interactions with immigration officials (e.g., asylum or visa applications), and detect imposters. When USCIS captures fingerprints for purposes of an FBI Fingerprint Check, the fingerprints are also sent to OBIM for enrollment in IDENT. OBIM emails USCIS reports of any fingerprint records that match existing IDENT holdings, including visa refusals, immigration-related enrollments, and watchlist records. These reports are often called “Day Forward Reports.” All reported matches in these reports are manually reviewed in adjudicating some benefit types, but not others. In addition to reviewing OBIM reports for matches, IO may conduct a manual IDENT check by entering an individual’s A-Number in IDENT to determine if the system contains a matching record. When USCIS conducts an IDENT check, USCIS records the check and its result in CAMINO. There is no electronic communication between CAMINO and IDENT.

DOD Systems

Automated Biometrics Identification System (ABIS)⁶⁰ The DOD ABIS is a biometric database containing information collected by DOD personnel stationed abroad. ABIS is the DOD central, authoritative multi-modal (i.e., fingerprint, palm, iris, face) biometric repository. ABIS is an enterprise solution that is the strategic level authoritative data source for unclassified DOD biometrics. It integrates the DOD worldwide biometric efforts targeting known and suspected terrorists. The system operates and enhances associated search and retrieval services and interfaces with existing DOD and interagency biometric systems. DOD may retain USCIS records pursuant to negotiated information sharing access agreements.

Defense Clearance and Investigative Index (DCII)⁶¹ The USCIS Form N-426 is required for all naturalization applicants who have had prior service in any of the branches of the U.S. Armed Forces. The Form N-426 is used to search military held records by running a Defense Clearance and Investigative Index (DCII) check. Each military branch has agreed to do this for members who have served or are currently serving their branch. Under the facilitated military N-400 filing procedure, the military will front-end the processing of the Form N-426 check. The N-400 will be submitted with this check already done and the results attached.

⁵⁹ See DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), available at www.dhs.gov/privacy.

⁶⁰ See Defense Biometric Services, September 22, 2009, 74 FR 48237, Department of Defense Detainee Biometric Information System (March 28, 2007, 72 FR 14534), and Defense Biometric Identification Records System (April 17, 2009, 74 FR 17840), available at <http://dpcl.d.defense.gov/Privacy/SORNs.aspx>.

⁶¹ See Defense Clearance and Investigations Index (DCII), Aug. 17, 1999, 64 FR 44704, available at <http://www.dss.mil/foia/v5-02.html>.



USCIS must conduct a DCII query with the DOD as part of the background check process on any applicant with military service regardless of the section of law under which he or she is applying for naturalization. DCII checks are conducted manually by DOD and then sent to USCIS. USCIS manually enters a record of those checks and their results are manually entered into CAMINO. There is no electronic communication between DCII and CAMINO.

DD Form 214, Certificate of Release or Discharge from Active Duty – Report of Separation is a report of separation that captures the dates and character of service (type of discharge) of the service member. The DOD issues DD Form 214 to each veteran upon his or her separation from the Armed Forces. DD Form 214 is already certified by the respective Armed Forces branch and therefore meets the military service certification requirements set forth in section 328 and 329 of the INA. If the subject has been discharged from military service, the personnel files are stored at NARA, which is the official repository for records of military personnel who have been discharged from the U.S. Air Force, Army, Marine Corps, Navy, and Coast Guard.⁶²

USCIS uses this information to determine naturalization eligibility. DD Form 214 checks are conducted manually by DOD and then sent to USCIS. USCIS manually enters a record of those checks and their results into CAMINO. There is no electronic communication between DOD and CAMINO for sharing the information on DD Form 214.

DOJ Systems

FBI Name Checks⁶³ involve processing research and disseminating information contained in 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 and national security purposes. The UNI consists of administrative, applicant, criminal, personnel, and other law enforcement files. FBI Research Analysts return pertinent derogatory information to USCIS. FBI Name Checks are typically initiated by a Service Center domestically, and USCIS manually records those checks and their results in CAMINO. The results of the FBI Name Checks are used to determine an applicant's eligibility for a USCIS benefit. There is no electronic communication between the FBI Name Check system and CAMINO.

⁶² See About Military Service Records and Official Military Personnel Files (OMPF, DD Form 214) at <http://www.archives.gov/veterans/military-service-records/about-service-records.html>.

⁶³ See FBI-002 FBI Central Records System, 72 FR 3410 (Jan. 25, 2007); FED. BUREAU OF INVESTIGATION, NAT'L NAME CHECK PROGRAM, <http://www.fbi.gov/stats-services/name-checks>.



Next Generation Identification (NGI)⁶⁴ houses local, state, and federal law enforcement information. NGI is the largest biometric database in the world, housing the fingerprints and criminal histories for more than 70 million subjects in the criminal master file, along with more than 34 million civil prints. Included in the criminal database are fingerprints from 73,000 known and suspected terrorists processed by the United States or by international law enforcement agencies who work with the FBI. USCIS uses NGI to conduct searches of an individual's fingerprints against its records. The results provide summary information of an individual's administrative or criminal record within the United States. NGI results are stored in CPMS. There is no electronic communication between CAMINO and the NGI system.

DOS Systems

Automated Biometric Identification System (ABIS)⁶⁵ enables Facial Recognition (FR) digital photos of individuals seeking immigration benefits to be scanned against a database of digital images maintained by the DOS Kentucky Consular Center consisting of past applicants for non-immigrant and immigrant visas and other digital photo sources. Computerized Face Recognition (FR) has the potential to recognize several photos of the same person in databases that are exponentially larger than those that a human could review. Additionally, automated FR can detect mathematical similarities that could be easily disguised from a subjective human viewer.

DOS initiates FR checks on behalf of USCIS in certain circumstances and then reports the results of the FR to USCIS. USCIS manually enters this information into CAMINO. There is no electronic communication between CAMINO and DOS FR software.

Consular Consolidated Database (CCD)⁶⁶ is a data warehouse that holds current and archived data from the DOS Consular Affairs (CA) domestic and post databases around the world. It was created to provide DOS CA a near real-time aggregate of the consular transaction activity collected domestically and at post databases worldwide.

USCIS conducts CCD checks manually and records those checks and their results in CAMINO. There is no electronic communication between CAMINO and CCD.

Consular Lookout and Support System (CLASS)⁶⁷ is a name-check database that contains records provided by numerous agencies and includes information on persons with visa refusals, immigration violations, criminal histories, and terrorism concerns, as well as intelligence information and child support enforcement data. In addition to containing information from DOS sources, sources for information in CLASS includes NCTC/TSC (terrorist watch lists),

⁶⁴ See FBI-009 Fingerprint Identification Records System (FIRS), 72 FR 3410 (Jan. 25, 2007).

⁶⁵ See Automated Biometric Identification System PIA, available at <http://www.state.gov/documents/organization/109132.pdf>.

⁶⁶ See Consular Consolidated Database (CCD) PIA, available at <http://www.state.gov/m/a/ips/c24223.htm>.

⁶⁷ See Consular Lookout and Support System (CLASS) PIA, available at <http://www.state.gov/m/a/ips/c24223.htm>.



DHS (TECS), Interpol, DOJ Drug Enforcement Agency, U.S. Department of Health and Human Services, and FBI (extracts of the NCIC Wanted Person, Immigration Violator, Foreign Fugitive Files, Violent Gang and Terrorist Organization File, and the Interstate Identification Index).

DOS initiates CLASS checks on behalf of USCIS in certain circumstances and reports the results to USCIS. USCIS manually enters the CLASS check results in CAMINO. There is no electronic communication between CAMINO and the DOS CLASS system.

Security Advisory Opinion (SAO)⁶⁸ is a name check conducted by DOS on certain categories of refugees, refugee and asylee beneficiaries, and visa applicants and identifies those with a criminal history or those who may pose a national security concern.

DOS reports the results to USCIS. SAO check results are manually updated in CAMINO. There is no electronic communication between CAMINO and the DOS system which initiates the SAO check process.

NCTC

NCTC's classified terrorism data holdings. Pursuant to the National Security Act of 1974, as amended, NCTC "serves 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."⁶⁹ On a regular basis, reports are pulled from CAMINO of individuals requiring a counterterrorism check. The list is then encrypted and sent to NCTC to check for possible matches to records in NCTC terrorism holdings. NCTC reports results back to IO HQ via email if no hit is found, or via a classified mechanism if a match is found. USCIS uses this information in support of its identification of terrorism-related inadmissibilities. The clear or not clear results of the NCTC check are batch uploaded into CAMINO. There is no electronic communication directly between CAMINO and the NCTC.

⁶⁸ See Visa Opinion Information Service (VOIS), available at <http://foia.state.gov/docs/PIA/185304.pdf>. See also STATE-39, Visa Records, 77 FR 65245 (Oct. 25, 2012).

⁶⁹ 50 U.S.C. § 404o.



APPENDIX D

Security Checks for Humanitarian Parole (HP), Significant Public Benefit Parole (SPBP), and Refugee/Asylee Follow-to-Join Applicants

DHS and NCTC established a pilot in 2011 to analyze various immigration benefit screening enhancements.⁷⁰ Portions of sharing arrangement are in place today, specifically vetting of HP, SPBP, and follow-to-join applications.⁷¹

Under terms and conditions reflected in a Memorandum of Agreement (MOA), USCIS has partnered with NCTC to determine if Terrorism Information⁷² exists in HP, SPBP, and follow-to-join applications, including information that would be a bar to admissibility⁷³ under the Immigration and Nationality Act.⁷⁴

The information about the HP, SPBP, and refugee/asylee follow-to-join applicants is pulled from newly received applications that have already been entered into CAMINO, and periodically shared with NCTC.

Data Elements:

Pursuant to the MOA, IO provides NCTC with a file, via encrypted electronic transmission in accordance with information security standards, with the following information about covered individuals: full name, alias(es), A-Number, date of birth, country of birth, country of nationality/citizenship, passport number, gender, mailing address, physical address, phone number, and email address for the covered petitioners, beneficiaries, or applicants.

Population:

The population for this pilot consists of new applications for humanitarian parole or significant public benefit parole received during the term of the agreement. It also includes

⁷⁰ ISAA-262-001, Memorandum of Agreement Between the Department of Homeland Security and the National Counterterrorism Center Regarding Pilots for NCTC to support to USCIS Screening of Applicants for Immigration Benefits, August 30, 2011.

⁷¹ Addendum IV to the August 30, 2011 Memorandum of Agreement Between the Department of Homeland Security and the National Counterterrorism Center Regarding Pilots for NCTC to support to USCIS Screening of Applicants for Immigration Benefits, August 4, 2014.

⁷² Terrorism Information is defined as, (A)... all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to— (i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (iii) communications of or by such groups or individuals; or (iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and (B) includes weapons of mass destruction information. 6 U.S.C. § 485

⁷³ Please visit the USCIS website for more information on HP, SPBP, and Refugee/Asylee and its requirements at www.uscis.gov.

⁷⁴ See 8 U.S.C. §§ 1182(a)(3)(A), (B), (F); 1227(a)(4)(A), (B).



information being processed for travel documents from refugee/asylee relative petitions received by USCIS international offices during the life of the pilot. The affected groups include individuals outside of the United States who are requesting parole or on whose behalf parole is being requested and their LPR or U.S. Citizen petitioners, and the spouses and unmarried children of refugees and asylees.

Individuals with asylum or refugee status, or those that do not have that status, but who may have applied for it at some point, may be among the pool of parole applicants and petitioners. Disclosure of asylum data (and also refugee data, which as a matter of DHS policy is treated in the same manner as asylum data) is authorized in accordance with 8 C.F.R. § 208.6 and the terms and conditions of the Memorandum from the Secretary of DHS entitled “Disclosure of Asylum-Related Information to U.S. Intelligence and Counterterrorism Agencies,” dated April 18, 2007, or any subsequently issued or superseding guidance issued by the Secretary or Deputy Secretary of Homeland Security. USCIS will not provide data pertaining to other special protected class individuals covered under 8 U.S.C. § 1367 to NCTC under the MOA.

Vetting:

NCTC analyzes USCIS data in conjunction with other data it holds to determine if the USCIS data provided under the MOA constitutes Terrorism Information. NCTC delivers the analytic results within 90 days of the notification by NCTC to USCIS that the data has been formatted and loaded by NCTC. If data is found to constitute Terrorism Information, NCTC will notify USCIS via unclassified email when such Terrorism Information exists and will provide USCIS with the associated report number, which USCIS can access through appropriate channels. National security-related information, including classified reports generated by NCTC, may be stored in the A-File.

Privacy Mitigation:

The MOA establishes the terms and conditions of NCTC’s access, use, and retention of HP, SPBP, and follow-to-join information. First, the MOA limits NCTC’s use of the data solely to analyzing it to determine whether it has a nexus to terrorism. The MOA then limits NCTC’s retention of HP, SPBP, and follow-to-join information to no longer than 150 days, after which it must be purged. This deletion timeframe provides NCTC with enough time to identify Terrorism Information and to coordinate with USCIS regarding any Terrorism Information found in HP, SPBP, or follow-to-join applications. If NCTC identifies Terrorism Information associated with HP, SPBP, or follow-to-join individuals, then NCTC may permanently retain, use, and disseminate the information consistent with its authorities.

The MOA also features protections against unauthorized dissemination of HP, SPBP, or follow-to-join information. NCTC is prohibited from further disseminating HP, SPBP, or follow-to-join information unless they first identify it as Terrorism Information or obtain written permission



from DHS, including review and approval by USCIS, the DHS Privacy Office, Office for Civil Rights and Civil Liberties, Office of the General Counsel, and Policy Office.

The MOA includes further privacy protections including requirements for training and recognition that both parties are participants in the Information Sharing Environment (ISE) and will adhere to their written ISE Privacy and Civil Liberties Protection Policy and have provisions for correction and redress. Finally, under the terms of the agreement, NCTC makes regular reports about its use of the HP, SPBP, and refugee/asylee follow-to-join data. These reports include the number of records reviewed; records initially identified as Terrorism Information; records confirmed to be Terrorism Information through human review and retained; the number of NCTC intelligence reports including covered information; the number of TIDE records enhanced with covered information; and the number of records deleted when their retention period expired. In addition to these regular reports, NCTC must also notify DHS of known or suspected failures to adhere to the MOA's terms and conditions.