Privacy Impact Assessment
for the

Refugees, Asylum, and Parole System and the Asylum Pre-Screening System

November 24, 2009

Contact Point
Donald Hawkins, Privacy Officer
United States Citizenship and Immigration Services
Department of Homeland Security
(202) 272-1513

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

Abstract

United States Citizenship and Immigration Services (USCIS), a component of the Department of Homeland Security (DHS), maintains the Refugees, Asylum, and Parole System (RAPS) and the Asylum Pre-Screening System (APSS). Both systems, originally developed by the former Immigration and Naturalization Service (INS), comprise the USCIS' Asylum program[1] and are used to capture information pertaining to asylum applications, credible fear and reasonable fear screening processes, and applications for benefits provided by Section 203 of the Nicaraguan Adjustment and Central American Relief Act (NACARA § 203).[2] USCIS has conducted this Privacy Impact Assessment (PIA) because both RAPS and APSS contain personally identifiable information (PII).

Overview

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

(1) immigrant petitions;

(2) non-immigrant petitions (petitions filed by persons staying in the US temporarily for a limited purpose (e.g., to work));

(3) asylum and refugee applications; and

(4) naturalization applications.

This PIA covers the USCIS Asylum Division processing program. This program is anchored by two information technology data systems: RAPS and APSS. Because RAPS and APSS' business and substantive functions are so closely aligned, CIS is addressing them in the same PIA.[3]

Authority and Need for RAPS and APSS

---

[1] It should be noted that, despite its name, no refugee or parole applicant records are stored in RAPS, although those immigration classifications were contemplated as part of RAPS's original design but never included operationally. dif

[2] Pub. L. No. 105-100, 111 Stat. 2193 (1997), *amended by* Pub. L. No. 105-139, 111 Stat. 2644 (December 2, 1997).

[3] The processing of immigrant and non-immigrant petitions are covered by another USCIS PIA entitled "USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum" (including the Computer Linked Application Information Management System [CLAIMS] 3 database). The processing of naturalization applications is covered by the PIA for CLAIMS 4. Both PIAs can be found at www.dhs.gov/privacy, following the links to "Privacy Impact Assessments."

As set forth in Section 451(b) of the Homeland Security Act of 2002, Public Law 107-296, Congress charged USCIS with the administration of the asylum program, which provides protection to qualified individuals in the United States who have suffered past persecution or have a well-founded fear of future persecution in their country of origin as outlined under INA § 208 and 8 CFR § 208. USCIS is also responsible for the adjudication of the benefit program established by Section 203 of the Nicaraguan Adjustment and Central American Relief Act (NACARA § 203) (discussed in more detail in Section B below), in accordance with 8 CFR § 240.60 and the maintenance and administration of the credible fear and reasonable fear screening processes, in accordance with 8 CFR §§ 208.30 and 208.31. USCIS developed RAPS and APSS in order to carry out its obligations in administering these benefit programs.

Functions

RAPS and APSS track case status and facilitate the scheduling of appointments and interviews and the issuance of notices (including receipt notices, appointment notices, and decision letters) at several stages of the adjudication process. USCIS Asylum Offices use RAPS and APSS to:

- record decisions and to generate decision documents such as approval, dismissal, or rescission of an asylum or NACARA § 203 application,
- denial of an asylum application,
- administrative closure of an asylum application, or
- referral of an asylum or NACARA § 203 application to Executive Office of Immigration Review (EOIR).

The systems also initiate, receive, and record responses for national security and background check screening and prevent the approval of any benefit prior to the review and completion of all security checks. Finally, the systems provide fully developed and flexible means for analyzing and managing program workflows and provide the Asylum Program with statistical reports to assist with oversight of production and processing goals.

RAPS

RAPS is a comprehensive case management tool that enables USCIS to handle and process applications for asylum pursuant to Section 208 of the Immigration and Naturalization Act (INA) and applications for suspension of deportation or special rule cancellation of removal pursuant to NACARA § 203. DHS offices worldwide can access RAPS as a resource of current and historic immigration status information on more than one million applicants. DHS officials can use RAPS to verify the status of asylum applicants, asylees, and their dependents to assist with the verification of an individual's immigration history in the course of a review of visa petitions and other benefit applications as well.

RAPS Typical Transaction

A typical transaction begins when an individual initiates the process to apply for asylum by completing and filing Form I-589, *Application for Asylum and for Withholding of Removal*, with a USCIS Service Center, or in certain circumstances directly with an asylum office. Service Center personnel receive the application in person or via mail and manually enter, most, but not all, of the information from a new application into RAPS.

Once the information is entered into the system, RAPS generates an appointment notice for the collection of fingerprints used to complete criminal and background checks and to create Employment Authorization Documents (EADs), as appropriate. The applicant will appear at a USCIS service center to provide fingerprints and confirm application information.

RAPS then automatically initiates several background security check processes: Federal Bureau of Investigation (FBI) Name Check, United States Visitor and Immigrant Status Indicator Technology (US-VISIT) and DHS' Automated Biometric Identification System (IDENT), Customs and Border Protection (CBP) TECS, FBI Fingerprint, and the ENFORCE Alien Removal Module (EARM) (for a full discussion of the background check process, see Section 5.1). RAPS also stores the results of security checks.

When a new application is entered into RAPS, it is forwarded to a USCIS Asylum Office for interview and adjudication.[4] Asylum Offices use RAPS to schedule an asylum interview to evaluate the claim of asylum status and to conduct various aspects of case maintenance such as address changes, updates of information pertaining to dependent claimants, to record preliminary and final decisions, and to generate decision documents. An individual who files for asylum may include in his or her application any spouse or child who is within the United States and appears for the asylum interview. This is because a grant received by the principal asylum applicant is conveyed to the spouse and children included in the family group if the spouse/child is in the U.S. and not otherwise barred from a grant of asylum.

RAPS also supports the implementation of Section 203 of NACARA, which provides that certain Salvadorans, Guatemalans, and nationals of former Soviet bloc countries, as well as their qualified relatives, may apply for relief from deportation or removal and, if granted, gain lawful permanent resident status. Certain individuals with pending asylum applications and their family members may also apply with USCIS for benefits under NACARA §203. Applicants must first establish eligibility to *apply* for NACARA § 203 relief and then demonstrate that they are eligible for *a grant* of relief. (Please visit the USCIS website at www.uscis.gov for details on NACARA § 203 eligibility criteria.) The typical transaction for a NACARA application is the same as a RAPS transaction except a different form is used.

Under NACARA § 203, a typical transaction begins when an individual initiates the process to apply for relief by mailing or hand delivering a completed Form I-881, *Application for Suspension of Deportation or Special Rule Cancellation of Removal*, to a USCIS Service Center. The Service Center then enters the application information into RAPS, which initiate background and security checks and automatically generates an appointment notice for the collection of fingerprints necessary to complete the background check process.

Once the USCIS Service Center has created the new RAPS record, the applicant's file is forwarded to a USCIS Asylum Office for the interview of the applicant and the adjudication of the application. Asylum Offices use RAPS to track the applications of family groups while preparing

[4] After the application is entered into the system, RAPS automatically calculates the amount of time the application has been pending. This calculation is important because asylum applicants who have not received a final decision from USCIS within 150 days of filing are eligible to apply for an EAD. The amount of time a petition is pending is adjusted to account for delays caused by the applicant. These adjustments are recorded in RAPS to prevent applicants from intentionally causing delays solely to obtain an EAD.

the application for adjudication and scheduling the applicants for interview. RAPS also enables USCIS to conduct regular file maintenance, record decisions, and generate the necessary decision documentation for issuance.

APSS

APSS is a case management system that supports USCIS in the screening of individuals in the expedited removal process [5] and of individuals subject to reinstatement of a final order of removal or an administrative removal order based on a conviction of an aggravated felony to determine whether they have credible fear or reasonable fear as defined by 8 CFR § 208.30 and 8 C.F.R. § 208.31.[6]

In both the credible and reasonable fear processes, APSS is used to record and track steps in the screening process, including asylum office determinations. When cases are entered into APSS by a USCIS Asylum Office, background and security checks are automatically initiated for the applicant. APSS has automated background check capability for the FBI Name Check and CBP TECS. Credible and reasonable fear determinations are recorded using the APSS case management system following the screening interview.

Thus, RAPS and APSS track case status and facilitate the scheduling of appointments and interviews and the issuance of notices (including receipt notices, appointment notices, and decision letters) at several stages of the adjudication process. USCIS Asylum Offices use RAPS and APSS to record decisions and to generate decision documents such as approval, dismissal, or rescission of an asylum or NACARA § 203 application, denial of an asylum application, administrative closure of an asylum application, or referral of an asylum or NACARA § 203 application to Executive Office of Immigration Review (EOIR). The systems also initiate, receive, and record responses for national security and background check screening and prevent the approval of any benefit prior to the review and completion of all security checks. Finally, the systems provide fully-developed and flexible means for analyzing and managing program workflows and provide the Asylum Program with statistical reports to assist with oversight of production and processing goals.

Section 1.0 Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

[5] Expedited removal is a provision under which an alien who lacks proper documentation or has committed fraud or willful misrepresentation of facts may be removed from the United States without any further hearings or review unless the alien indicates a fear of persecution or torture or an intention to apply for asylum. See INA §235.

[6] An alien is found to have a credible fear when there is a significant possibility that the alien could establish eligibility for asylum or protection under the *Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment* ("*Convention Against Torture*"). .8 U.S.C. 1158; 8 C.F.R. § 208.30(e)(3). An alien is found to have a reasonable fear when there is a reasonable possibility that the alien could establish eligibility for protection under the *Convention Against Torture* or could merit other consideration by an immigration judge. 8 C.F.R. § 208.31

RAPS and APSS contain the following personal data elements for the following purposes:

Names: USCIS collects names (First, Last, and Middle) and aliases for principal applicants, family members, also known as derivatives, and the preparer of the application in RAPS and APSS. Contact information of the attorney or representative is not captured in RAPS as this is available in the Private Attorney Maintenance System (PAMS). (See section 4.1 for a full discussion of PAMS.)

Information Regarding Immigration Status: USCIS collects information relating to immigration status such as A-Numbers, port and date of entry, status at entry, filing date of asylum application, basis of eligibility, interview location, encounter location (i.e., where an Asylum Officer first encounters the individual), immigration court, deportation information, employment authorization eligibility and application history, case status, and case history in certain forms and enters them into RAPS and APSS as part of the application process for asylum, NACARA, credible fear and reasonable fear.

Addresses: USCIS collects the addresses of applicants and/or application preparers in RAPS and APSS. In addition, USCIS collects this information to substantiate an applicant's claim of continuous residence in the U.S. as required to establish eligibility in some applications. For APSS records, if the applicant is in detention, the detention facility's address is recorded. The addresses of applicant's dependents are not included in RAPS unless they have applied separately as a principal asylum or NACARA 203 applicant.

Telephone Numbers: USCIS collects telephone numbers of the applicant and preparer in order to have a secondary means of contacting either when needed to collect or provide information. The contact numbers of applicant's dependents are not included in RAPS unless they have applied separately as a principal asylum or NACARA § 203 applicant.

Birth Dates: USCIS collects birth dates (applicant, petitioner, spouse, children/stepchildren/adopted children) and enters them into in RAPS and APSS.

Social Security Numbers: USCIS collects Social Security numbers (applicant and spouse) and enters them into RAPS and APSS.

Citizenship/Nationality/Religion Information: USCIS collects information on the applicant's country of nationality, country of birth, ethnic origin, province of residence in home country, languages spoken, and religion.

Marital Status: USCIS collects information regarding marital status (i.e., whether applicant is married, single, widowed, or divorced) and enters this information into RAPS and APSS.

Gender: USCIS collects the genders of the applicant and dependents and enters them into RAPS and APSS.

Results of Background Security and Identity Checks Queries of background and security check systems based on name and date of birth or biometrics return results for newly filed applications and whenever a check is reinitiated to renew an expiring check or prior to a decision. Each check and law enforcement system is described in detail in Section 4.1, and briefly summarized below.

- **CBP TECS check** – A check on the applicant's name and date of birth returns a positive or negative response to RAPS or APSS. The response will be displayed in RAPS or APSS as a positive or negative match. This check can be renewed manually.
- **ENFORCE Alien Removal Module (EARM) check** – A check on the applicant's name and date of birth returns a positive or negative response to RAPS only. The response will be displayed in RAPS as a positive or negative match. This check can take place through the automated interface one time only.
- **FBI Fingerprint check** – A check on the applicant's ten-print biometrics returns the date of the applicant's fingerprint appointment at an USCIS Application Support Center (ASC), the date that the biometrics are sent to the FBI, and the date and the result of the check. The response will be displayed in RAPS as a positive or negative match. This check can be renewed manually via RAPS.
- **FBI Name check** – A check on all names and dates of birth used by the applicant return a positive or negative response to RAPS and APSS. The response will be displayed in RAPS or APSS as a positive or negative match for each alias and alternate date of birth.
- **US-VISIT/IDENT check** – A check on the applicant's ten-print biometrics returns the applicant's identification number assigned by US-VISIT/IDENT, the dates that the information is collected and uploaded to the system, and the nature of the hit (whether the hit is of a law enforcement nature), if any. New information uploaded to US-VISIT/IDENT will appear in the applicant's system record if it is of a higher law enforcement interest than prior hits.

Background and security check results are uploaded to RAPS during a nightly update. The results of checks are also included on reports automatically generated at each Asylum Office listing individuals flagged as potential "hits." Most security checks expire or are limited in verification for a specific application; therefore, RAPS allows checks to be reinitiated as necessary. It should be noted that RAPS does not contain all information provided in the I-589 or I-881, such as descriptive narratives related to the basis of the claim and information on the applicant's educational background and past addresses. Also, no biometric data or photographs are stored in RAPS.

Preparers: Data on individuals who prepared the asylum application are collected in RAPS. This information is not collected in APSS.

Relatives: Spousal and parent-child relationships are collected. In RAPS NACARA § 203 cases, relationship information may be entered to support the applicant's eligibility.

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

A majority of the data in RAPS and APSS is obtained directly from the individual applicant. Information regarding an applicant's spouse and children included in the application will also be housed in both RAPS and APSS.

RAPS also receives continuous updates from US-VISIT/IDENT on records related to the subjects of asylum applications that are entered in the US-VISIT Secondary Inspection Tool (SIT) and contained within the Watch List or US-VISIT IDENT databases. The initial updates of US-VISIT on asylum applicants (the "Search and Enroll" encounter) are usually the result of processing by

the ASC, which forwards records to US-VISIT. Records of basic information including name, encounter ID, and hit information, in turn, are uploaded to RAPS. In addition, records on any subsequent encounters with subjects of an asylum application are uploaded to RAPS by US-VISIT.

CBP's TECS, ICE's ENFORCE, and US-VISIT's IDENT systems all contribute background check determinations to RAPS and APSS. For more detail on those systems see Question 4.1.

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

The information in RAPS and APSS is collected to facilitate case processing and to maintain an electronic retrieval system containing information related to the status of asylum applicants. The specific purpose for collecting each data element is contained in Section 1.1 of this PIA.

RAPS and APSS support the business requirements of USCIS by providing the following major capabilities:

- Enabling the USCIS Asylum Division to intake and process individual applications such as scheduling interviews, tracking case status, initiating and facilitating security checks, and generating notices and decision letters;
- Providing fully-developed and flexible tools for analyzing and managing program workflows locally and nationwide;
- Enabling USCIS personnel to promptly access accurate biographical and class of admission/status information on benefit applicants to ensure proper identification and adjudication;
- Providing statistical reports to USCIS, other government agencies, and certain public interest groups; and
- Enabling the Asylum Division to self-monitor areas of progress and program issues that require attention or action.

1.4 How is the information collected?

The data in RAPS and APSS is generally obtained directly from the individual requesting benefits, entered manually by Asylum Office staff, and augmented with updates[7] by staff and from other systems as discussed in Section 4.1 and 5.1. The information is largely obtained from the OMB-approved Form I-589, *Application for Asylum and for Withholding of Removal* (OMB No. 1615-0067) and Form I-881, *Application for Suspension of Deportation or Special Rule Cancellation of Removal* (Pursuant to Section 203 of Public Law 105-100, NACARA) (OMB No. 1615-0072) and through applicant interviews. CIS collects information regarding background checks electronically.

1.5 How will the information be checked for accuracy?

[7] Asylum Office staff review the data in RAPS for data entry mistakes and for fields that have not been updated. To complete the review, staff may check CIS, CLAIMS-3, and US-VISIT/IDENT. Data missing from the interfaces described in the Technology section above may also be updated with information found within the relevant systems.

All applicants within the jurisdiction of an Asylum Office receive a personal interview prior to the full adjudication of his or her benefit application. Applicant information contained in RAPS and APSS is checked for accuracy by an Asylum Officer through this interview process. The RAPS and APSS record for each case is subject to 100 percent supervisory review prior to a final determination. Records are also subject to review by Asylum Division Headquarters for cases which require quality assurance review according to asylum procedures. The applicant's information (including biographical data, claim and immigration history) is verified and, if necessary, corrected on the form as well as in RAPS and APSS based on any new information obtained during the interview or to correct errors found during supervisory or headquarters review.

Standard operating procedures direct Asylum Offices in correctly entering applicant data and decision processing information. These operating procedures include the following:

- *Affirmative Asylum Procedures Manual, publicly available at www.uscis.gov;*
- *ABC / NACARA Procedures Manual;*
- *Reasonable Fear Procedures Manual;*
- *Credible Fear Procedures Manual;*
- *Identity and Security Checks Procedures Manual; and*
- *Procedures for the Automated Generation of the I-766 Employment Authorization Document in the Asylum Process.*

RAPS and APSS are designed to require specific entries in the sequence outlined by the operating procedures to prevent inconsistencies in applicant data and in decision processing entries. RAPS and APSS accomplish this through program coding that allows or prevents record updates based on defined parameters. Therefore, for any security check that must be completed prior to an interview or a final decision, the systems will prevent an entry prior to the completion of the security check. Similar edits exist for case closures, case transfers, file maintenance, and many other case processing tasks. Furthermore, standard reoccurring reports are generated to identify cases that are pending due to incomplete record updates. The reports are used to identify and correct or complete the record updates to allow for proper and timely case completion.

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

The authority to collect information in RAPS and APSS is set forth in the Immigration and Nationality Act, 8 U.S.C. §§ 1103, 1158, 1225, 1228, and Title II of Public Law 105-100 and in the implementing regulations found in volume 8 of the Code of Federal Regulations (CFR).

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy Risk: Unauthorized access to information.

Mitigation: The user interface for RAPS and APSS is available only via specific government-owned hardware or using a government-issued security token. USCIS offices where these specific consoles are available are located in buildings staffed with 24-hour security service and other security mechanisms, and access to premises is restricted to those provided official identification and authorization. All records are stored in spaces that are locked after normal office hours. Paper records are stored in secured areas that are locked outside of normal office hours. The specific user must have been provided the proper user roles to view RAPS or APSS before the systems are visible through the user interface.

Privacy Risk: Data inaccuracy.

Mitigation: All data that is entered into RAPS and APSS is confirmed by a USCIS Asylum Officer during the applicant interview and by a USCIS Supervisory Asylum Officer during the quality assurance review required for all cases. For those applicants who fail to appear for the interview, Asylum Office personnel check the data in RAPS against what was provided in the application prior to the administrative closure of the application for failure to appear.

Privacy Risk: Obtaining more data than necessary during the course of the application and interview processes thus violating the Privacy Act data minimization requirements.

Mitigation: RAPS and APSS allow the entry of only the minimum data required to conduct a full asylum interview and complete the benefit adjudication. All personal data is entered using the data entry commands, which are configured to match the questions asked in the applications, such as the *Application for Asylum and for Withholding for Removal*, Form I-589. All information requested in the applications is relevant to ensure that all bona fide applicants are identified, to prevent benefit fraud, and to enable offices to adjudicate and deliver/serve decisions at the individual's appropriate address.

The data collected in RAPS and APSS is used by Asylum Officers who have a duty to elicit all testimony that may demonstrate benefit eligibility. For example, an applicant may be eligible for asylum if the applicant has a well-founded fear of persecution on account of his or her race, religion, nationality, membership in a particular social group, and/or political opinion. Although applicants may demonstrate eligibility under any one of the five categories, an asylum officer records in RAPS each protected category claimed by the applicant. The resulting record is then considered during the mandatory supervisory review and possible review by Asylum Division Headquarters.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

All of the information in Question 1.1 is used to:

- correctly record and identify the applicant and to verify the accuracy of information provided in an application (including the information of spouses and dependents),

- send correspondence (e.g., denial, grant and/or requests for additional information) to the applicant or other persons relevant to the application process, and

- verify with the applicant any assistance received in the completion of the application to assist in tracking and investigating preparer fraud.

USCIS uses the information to manage, control, and track the process of affirmative asylum applications, applications for suspension of deportation/special rule cancellation of removal pursuant to Section 203 of NACARA, as well as credible fear and reasonable fear screenings.

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

Data from RAPS and APSS are not used in complex analytical tools resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. RAPS and APSS do not create or make available new or previously unutilized information about an individual that would be placed in the individual's existing record.

Basic query reporting in RAPS and APSS is primarily used to track USCIS workflows and the productivity of adjudicating offices. Reports on applicants are used to investigate benefit fraud and cases of national security concern based on requests from the Fraud Detection and National Security Data System (FDNS).[8] No reporting or data manipulation is used to make eligibility determinations. All determinations of eligibility are made following a full review of the individual benefit application by an Asylum Officer and are subject to 100-percent supervisory review.

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

No commercial or publically available information is stored in RAPS or APSS. During the course of any adjudication, Asylum Office staff may use commercial record systems such as LexisNexis Law Enforcement Systems, Accurint, and ChoicePoint's AutotrackXP to investigate the veracity of a benefit application. None of these systems transmit data to or from RAPS or APSS.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Privacy Risk: Inappropriate use of information

Mitigation: Only personnel with the proper security clearance and a need for the information will be granted access to RAPS and APSS. The system administrator is responsible for granting the appropriate level of access. All USCIS employees and external government users will be properly trained on the use and release of information in accordance with agency policies,

[8] PIA published on July 29, 2008 at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_fdns.pdf

procedures, regulations, and guidance. In addition, USCIS personnel are required to take annual computer security awareness training.

Privacy Risk: Data Quality

Mitigation: The *USCIS Affirmative Asylum Procedures Manual* instructs Asylum Offices to review and update RAPS information for accuracy and completeness. USCIS has a number of procedures in place to check the accuracy of information coming into RAPS and APSS, including standard field and relational edits (e.g., ZIP codes and internal CIS mainframe tables verify that the appropriate state has been selected). Authorized USCIS personnel have the ability to correct inaccuracies brought to their attention internally, as well as by members of the public, which occurs during the course of the initial in-person interview with the applicant and at the time of decision pick-up. Individuals may request the correction of information contained within their files by submitting a Privacy Act request. For more information, including procedures regarding restrictions on protected access, see Section 7.

Section 3.0 Retention

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

3.1 How long is information retained?

NARA approved the following USCIS schedules for retention and disposal of RAPS and APSS records (RAPS N1-563-04-6 and APSS N1-563-04-7):

Automated A-File records will be maintained for 25 years after the case is closed, and then archived at the DOJ Data Processing Center or its designated successor for 75 years and then destroyed. Copies of system data may be stored in the individual's paper A-File (NCI-85-80-5/1). USCIS retains information generated by RAPS and APSS reports for only as long as is necessary to support the agency's mission. Reports are never archived longer than the approved retention schedule period.

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

The retention schedules were approved by NARA on September 16, 2003, for RAPS and November 3, 2003, for APSS.

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

Risk: Retaining information longer than necessary may exceed the limitations provided by the Privacy Act data minimization requirements.

Mitigation: All data and electronic images are being retained for the indicated periods to fulfill the business requirements of DHS and in accordance to the limits of the retention schedules, which includes adjudication of decisions, law enforcement uses, protection of national security, responding to requests within DHS, as well as those requests from other government agencies requiring historical and/or biographical information on the individuals of interest.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within DHS.

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

USCIS provides the following non-USCIS DHS components read only access to RAPS and APSS: (1) Customs and Border Protection (CBP), for border and inspection processing (to confirm immigration status); and (2) Immigration and Customs Enforcement (ICE), for investigatory, deportation, and immigration court functions. RAPS and APSS are also used to conduct queries for DHS law enforcement intelligence analysts upon request.

Other DHS agencies that may receive RAPS and APSS information on a case by case, *ad hoc* basis include the following components:

- The Office of Inspector General may be given RAPS and APSS information during the course of an audit, investigation or inspection.
- Office of Legislative Affairs may be given information in the course of in inquiry.
- Office of Citizen and Citizenship and Immigration Services Ombudsman may be given information in the course of an inquiry lodged by an applicant.
- Office of the General Counsel may be given information in the course of an investigation, litigation, or an assessment of a legal issue.
- Office of Policy may receive information in the course of an applicant's inquiry or an inquiry made by the DHS Secretary.
- Law enforcement actions, national security concerns or applicant inquiries, audits and inquiries by the DHS Secretary may require the release of RAPS and APSS information to other DHS components on an ad hoc basis.

Biographic information available on RAPS and APSS and statistical reports may be shared with the above-listed DHS components for the purposes of evaluating eligibility for a benefit, litigation and policymaking.

Information Shared Through Interfaces With Other DHS Systems:

USCIS SYSTEMS:

CLAIMS 3. RAPS sends a file daily to CLAIMS 3 with records on individuals that includes biographic information, a biometric receipt number, and the application approval date for all granted asylum applicants who are eligible to receive a secure two-year work authorization document. CLAIMS 3 processes the RAPS-generated request. CLAIMS 3 sends a nightly file of the

day's transactions with respect to individuals with a current status of Pending Asylum or Asylee. RAPS processes these records to update employment status and also address data if it is different from the current address already stored in RAPS. Beyond this, if the address update is applied to a case that was closed because the applicant failed to appear for interview or correspondence with the applicant was returned for bad address, the case is automatically reopened and the applicant is scheduled for interview.

Central Index System (CIS). There are four transmissions performed by the RAPS interface with the Central Index System. (1) A file is sent nightly adding new records to CIS for people added to RAPS during the day who were issued a new A-Number; (2) a file is sent nightly to CIS on people added during the day who already had an existing A-Number so that the status of the individuals can be changed to "Pending Asylum"; (3) a file is sent nightly requesting the transfer of the A-Files of the applicants/dependents with an existing A-Number to the owning Asylum Office; and (4) a file is sent nightly with the new status of individuals following final decision, e.g., asylee ("AS") in the case of a grant, or reversion to prior non-immigrant status in the case of a denial or administrative close.

Private Attorney Maintenance System (PAMS). Rather than redundantly storing data on attorneys representing asylum applicants, RAPS links to PAMS, a shared attorney resource on the CLAIMS-3 mainframe, and stores only the Attorney ID, a nine-byte value that uniquely identifies the attorney. The attorney ID is used to retrieve attorney data for purposes of display in RAPS and for creating attorney copies of all correspondence with the applicant.

National File Tracking System (NFTS). NFTS is an enhanced version of the Receipt and Alien File Accountability and Control System (RAFACS) and will eventually replace it altogether in USCIS offices throughout the country. NFTS is used by staff at the Asylum Offices to upload to RAPS and the Central Index records on the receipt of A-Files. NFTS is also used to print RAPS reports (e.g., interview schedule, decision pick-up schedule) in "Responsible Party Code" order to facilitate the aggregation of A-Files.

CLAIMS 4. RAPS submits records nightly to a scheduling module in CLAIMS 4 on individuals to be scheduled for processing at Application Support Centers (ASCs) for collection of photographs, fingerprints, and signatures. CLAIMS 4 confirms the scheduling, generates call-in notices, and returns the notices to RAPS.

USCIS Enterprise Service Bus (ESB) Person Centric Query Service (PCSQ). PCQ Service allows USCIS users to search for applicant records from multiple DHS systems that includes but is not limited the Central Index System (CIS), CLAIMS 3, CLAIMS 4, and the Enforcement Integrated Database (EID). USCIS has developed an interface between the Enterprise Service Bus and RAPS that allows officers of the USCIS National Security and Records Verification Directorate and Refugee, Asylum, and International Operations Directorate to review limited data on individuals with RAPS records. The use of PCQS will be limited to immigration status verification.

OTHER DHS SYSTEMS:

United States Visitor and Immigrant Status Indicator Technology (US-VISIT). RAPS receives continuous updates from US-VISIT/IDENT on records related to the subjects of asylum applications that are entered in the US-VISIT Secondary Inspection Tool (SIT) and contained within the Watch List or US-VISIT IDENT databases. The initial updates of US-VISIT on asylum applicants

(the "Search and Enroll" encounter) are usually the result of processing by the ASC, which forwards records to US-VISIT. Records of basic information including name, encounter ID, and hit information, in turn, are uploaded to RAPS. In addition, records on any subsequent encounters with subjects of an asylum application are uploaded to RAPS by US-VISIT.

ENFORCE Alien Removal Module (EARM). RAPS queries the EARM nightly to determine the presence of a record on all individuals added to RAPS during the day. Based on the returned file of potential "hits," RAPS (1) updates the individual's RAPS record to show an unresolved potential hit as a "Y" and (2) produces a report at the Asylum Office listing of individuals who must be checked further in EARM. Following this on-line query based on the findings of the batch search, Asylum Office staff update RAPS to show that the potential hit has been resolved, and the case can then be processed to completion. RAPS updates EARM with any new Notice to Appear for Removal Proceedings (NTA) issued to an asylum applicant.

DHS CBP TECS: TECS queries based on name and date of birth are conducted nightly on all individuals and added to RAPS during the day. A report with the results returned is generated at the Asylum Offices listing individuals flagged as potential "hits" in TECS. As with the EARM interface, a flag is put on the records of potential "hits" that prevents entry of a final decision until resolution of the TECS status is update in RAPS.

4.2 How is the information transmitted or disclosed?

Capabilities exist to transfer information through either encrypted electronic transmission or via paper (i.e., e-mail, disk, fax, telephone, or mail). The transfer of data by portable media is encrypted as required by Office of Management and Budget (OMB) Memorandum 06-16.[9]

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risk: The primary risk is unauthorized access to, or disclosure of, information contained within the systems.

Mitigation: Information in RAPS and APSS is safeguarded in accordance with applicable laws, rules, and policies as discussed in more detail below.

Confidentiality Provisions of 8 CFR § 208.6[10]:

Asylum-related data, in particular, is governed by strict regulatory confidentiality provisions outlined in 8 CFR § 208.6, Disclosure to Third Parties. This regulation generally

[9] OMB Memorandum 06-16 can be found at: http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf.

[10] http://www.uscis.gov/files/pressrelease/FctSheetConf061505.pdf

prohibits the disclosure to third parties of information contained in or pertaining to asylum applications, credible fear determinations, and reasonable fear determinations -- including information contained in RAPS or APSS -- except under certain limited circumstances. This regulation safeguards information that, if disclosed publicly, could subject the claimant to retaliatory measures by government authorities in their home country or non-state actors in the event that the claimant is repatriated, or endanger the security of the claimant's family members who may still reside in the country of origin. Moreover, public disclosure might give rise to a plausible protection claim where one would not otherwise exist by bringing an otherwise ineligible claimant to the attention of the government authority in the applicant's home country or a non-state actor against which the claimant has made allegations of mistreatment.

According to established interpretative guidance, confidentiality is breached when information contained in or pertaining to an asylum application (including information contained in RAPS or APSS) is disclosed to a third party in violation of the regulations, and the unauthorized disclosure is of a nature that allows the third party to link the identity of the applicant to: (1) the fact that the applicant has applied for asylum; (2) specific facts or allegations pertaining to the individual asylum claim contained in an asylum application; or (3) facts or allegations that are sufficient to give rise to a reasonable inference that the applicant has applied for asylum. The same principles govern the disclosure of information related to credible fear and reasonable fear determinations, as well as to applications for withholding or deferral of removal under Article 3 of the Convention against Torture, which are encompassed within the asylum application.

In the absence of the asylum applicant's written consent or the DHS Secretary's specific authorization, disclosure to third parties may be made only to United States government officials or contractors and United States federal or state courts on a need to know basis related to certain administrative, law enforcement, and civil actions. In some instances, interagency arrangements have been established - such as the arrangement between the former INS and the FBI -- to facilitate the proper disclosure of asylum-related information to United States agencies pursuant to the regulations. The release of information relating to an asylum application, credible fear determination, or reasonable fear determination (including information contained in RAPS or APSS) to an official of another government or to any entity for purposes not specifically authorized by the regulations without the written consent of the claimant requires the express permission of the DHS Secretary.

Privacy Safeguards of DHS and USCIS:

All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards that include restricting access to authorized personnel who have a need to know. This adheres to requirements of the DHS Information Technology Security Programs Handbook to employ password protection identification features to protect sensitive information. All internal components are mandated by DHS to comply with DHS' Sensitive System Security guidelines.

USCIS personnel are trained on how to interpret and use immigration information. USCIS personnel will explain the meaning of information contained within RAPS and APSS to non-immigration trained personnel in other DHS agencies prior to the dissemination of immigration related information contained within RAPS and APSS.

USCIS, ICE, and CBP personnel are trained to interpret and properly use immigration information through the use of web-based system training, INA training, and other miscellaneous on-the-job training received per their specific role. USCIS, ICE or CBP personnel are instructed to provide information regarding the restrictions of further disclosure prior to providing information contained within RAPS/APSS to non-immigration trained personnel in other DHS agencies. See Section 4.1 for a listing of DHS agencies.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local governments, and the private sector.

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

Information contained within RAPS and APSS may be shared with outside entities, either pursuant to regulation or through specific agreements. System records may be shared with the FBI and any other United States Government official or contractor having a need to examine information in connection with any United States Government investigation concerning any criminal or civil matter. In addition, information contained within RAPS and APSS may be shared with the FBI and the Intelligence Community for the purpose of gathering foreign counterintelligence or international terrorism information unrelated to pending criminal or civil litigation.

The DHS Secretary has also exercised his discretion to permit regular sharing of asylum-related information with the government of Canada. The arrangement is in the form of a *Statement of Mutual Understanding on Information Sharing* (SMU) and an Annex to the SMU, which together permit Canada's Department of Citizenship and Immigration Canada (CIC) and USCIS to exchange asylum-related records on both a case-by-case and systematic basis.

Information contained within RAPS and APSS may be shared with the government of Canada for the purpose of enhancing the ability of both the United States and the Canadian government to prevent abuse of the asylum process in their respective countries and to make accurate asylum eligibility determinations, thereby strengthening the integrity of both countries' asylum systems. The Secretary has authorized similar disclosure under agreements with the United Kingdom and Australia for specific projects.

In addition, in 2002, the Attorney General authorized the Asylum Division to release to the Office of Refugee Resettlement (ORR) of the Department of Health and Human Services (HHS) RAPS records for individuals granted asylum to enable ORR to meet congressional reporting requirements, provide more effective post-decision services, and generate statistical reports used to allocate funding for asylee social benefits. The electronic asylee data provided to the ORR will consist of the name, date of birth, alien number, gender, marital status, country of birth, country of citizenship, date of entry or admission into the United States, date of asylum grant, current city of residence, state of residence, street address, and zip code, as available.

In 2001, the Attorney General had also authorized the Asylum Division to disclose to HHS certain biographical information on asylees to enable ORR and the Centers for Disease Control (CDC) to provide emergency relief to qualified asylees. History records are created in RAPS on key updates received from EOIR on referred cases, i.e., acknowledgment of the Notice to Appear (NTA) receipt, date of scheduled hearing on the merits, and final decision.

USCIS and the United States Department of State are currently designing an interface to allow Department of State personnel to review limited RAPS records through the PCQ Service. PCQ will allow Department of State users to search for applicant records in RAPS as well as other USCIS systems of record. The access is to be provided as an addendum to pre-existing Memorandum of Understanding (MOU) between the Bureau of Consular Affairs, the Department of State and DHS USCIS, for the exchange of visa and immigration data.

Finally, the Attorney General and the DHS Secretary have, in rare circumstances, authorized disclosure on specific asylum seekers on a case-by-case basis to other U.S. government offices, foreign governments, and members of Congress. If the chair of a congressional committee with competent jurisdiction submits a written request for protected asylum-related information, then the requested information is generally provided without regard to the regulation. Written requests for asylum-related information by individual members of Congress or their respective staff members are considered on a case-by-case basis.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The current System of Records Notice (SORN) for this system was published in the Federal Register simultaneously with the publication of this PIA. It can be found at _____. The routine uses, which identify the manner in which RAPS and APSS are shared externally, are listed in the SORN. All sharing is compatible with the purpose for which the information was originally requested.

DHS personnel with immigration expertise may also provide information contained in the system to external organizations that meet the criteria outlined in 8 CFR § 208.6 or that are covered by a specific MOU or other agreement. USCIS has entered into a number of MOUs with various entities external to DHS to share information contained within RAPS and APSS. These documents dictate the terms and conditions for the release of relevant information as well as the appropriate use and safeguarding of all information.

Specific non-Asylum Office users within DHS, with a need-to-know, have read-only access to information contained within RAPS and APSS (e.g., USCIS staff overseas, USCIS Service Center personnel and CBP Officers). However, capabilities also exist to transfer information either through encrypted electronic transmission or via paper (i.e., e-mail, disk, fax, telephone, or mail).

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

For any non-Asylum user described in Section 5.2 above, measures are taken to ensure understanding of and compliance with the Privacy Act and 8 CFR 208.6. Federal government employees and their agents must adhere to the OMB guidance provided in OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, dated June 23, 2006, which sets forth the standards for the handling and safeguarding of PII. Non-Asylum Office users of the RAPS and APSS systems must sign non-disclosure agreements that dictate the confidentiality afforded to any accessed PII.

For users that are not employees of the USCIS Asylum Division, user roles are limited to read-only access. For all DHS users who are not employees of USCIS, CBP, or ICE, access to the system must be justified by the requesting office and must be necessary to the job duties of the potential new users. The Asylum Division proactively offers to provide in-person training for first-time users and is willing to provide training upon request.

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

Privacy Risk: Unauthorized access to information or unlawful disclosure

Mitigation: The primary risk is unauthorized access to, or disclosure of, information. To mitigate the risk, Asylum Division personnel strictly control the process of data sharing. As noted in 5.1, 5.2, and 5.3 above, all prospective users must be authorized to gain access to information contained within RAPS and APSS. All users who are not employees of the Refugee, Asylum, and International Operations Directorate must sign a non-disclosure agreement, which outlines the limits and restrictions regarding use of the data, prior to accessing the systems or viewing records contained by the system. Risks are further mitigated by provisions set forth in MOUs with federal and foreign government agencies. United States Government employees must undergo annual security awareness training.

Privacy Risk: Information security

Mitigation: USCIS has adopted the following information security practices to ensure information security: federal agencies are located in buildings with controlled access by security guards or authorized contractors for the government. Individuals gaining access to premises are required to have official identification. Information in RAPS and APSS is also safeguarded in accordance with applicable laws, rules and policies. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards including restricting access to authorized personnel who have a need-to-know. RAPS and APSS are maintained at Justice Data Center (JDC)-Dallas. Physical controls at the facility (e.g., guards, locks, etc.) have been implemented to prevent entry by unauthorized entities. Users have access to the databases by the use of, alpha-numeric passwords requiring at least one special character that must be changed every 60-days. Users are required to take security awareness training annually. Finally, RAPS and APSS do not contain classified information.

Privacy Risk: Inappropriate Use of Personally Identifiable Information (Social Security number, A-number, etc.)

Mitigation: USCIS provides access to the system only to individuals who have a specific need to know for the purpose of their job. Risks are further mitigated by provisions set forth in MOUs with federal and foreign government agencies. United States Government employees must undergo annual computer security awareness training.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

A System of Records Notice (SORN) for RAPS and APSS will be published in the Federal Register simultaneously with the publication of this PIA.

Individuals who apply for USCIS benefits are presented with a Privacy Act Statement as required by Section (e)(3)[11] of the Privacy Act and sign a release authorization on the benefit application/petition. The Privacy Act Statement details the authority to collect the information requested and the uses to which USCIS will put information the applicant provides on immigration forms and supporting documentation. The application forms also contain a provision by which an applicant authorizes USCIS to release any information received from the applicant as needed to determine eligibility for benefits.

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

Providing information on immigration forms is a voluntary act on the part of the individual seeking a benefit. Applicants can decline to provide information; however, the information contained in RAPS and APSS is requested from immigration benefit applicants to properly adjudicate their application. If the applicant does not wish to provide information to USCIS, his or her request for immigration benefits may be denied.

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

An applicant provides consent by virtue of applying for a USCIS benefit. The I-589 and the I-881, which are OMB approved applications, contain the following statements, which ask the

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

applicant to provide DHS with the written authority to release information provided by the applicant to assist in the determination of eligibility for the requested benefit:

> *I certify, under penalty of perjury under the laws of the United States of America, that this application and the evidence submitted with it are all true and correct. Title 18, United States Code, Section 1546(a), provides in part: Whoever knowingly makes under oath, or as permitted under penalty of perjury under Section 1746 of Title 28,United States Code, knowingly subscribes as true, any false statement with respect to a material fact in any application, affidavit, or other document required by the immigration laws or regulations prescribed thereunder, or knowingly presents any such application, affidavit, or other document containing any such false statement or which fails to contain any reasonable basis in law or fact - shall be fined in accordance with this title or imprisoned for up to 25 years.*
>
> *I authorize the release of any information from my immigration record that U.S. Citizenship and Immigration Services (USCIS) needs to determine eligibility for the benefit I am seeking.*

The SORN also notifies the individual of limitations on the right to consent to particular uses of the information because the information is released in the course of an investigation into fraud or a national security concern. The routine uses in the SORN notify individuals of external agencies with which APSS and RAPS share personal information.

In addition, an applicant may provide written consent to USCIS to allow disclosure to third parties with whom information cannot otherwise be shared pursuant to the regulations of 8 CFR 208.6.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

The extent of notice and opportunity to provide informed consent varies based on the particular purpose associated with the original collection of the information. In most cases, notice is provided when the applicant fills out the form or application for benefits. See Section 6.3.

Applicants for USCIS benefits are made aware that the information they are providing is being collected to determine whether they are eligible for immigration benefits. Each immigration form contains a provision by which an applicant authorizes USCIS to release any information from the application as needed to determine eligibility for benefits. Applicants are also advised that the information provided will be shared with other federal, state, local, and foreign law enforcement and regulatory agencies during the course of the investigation. The SORN provides additional notice to individuals by specifying the routine external uses to which the information will be put. In the USCIS website Privacy Notice, individuals are also notified that electronically submitted information is maintained and destroyed according to the principles of the Federal Records Act, NARA regulations and records schedules, and in some cases may be covered by the Privacy Act and subject to disclosure under the Freedom of Information Act (FOIA). OMB approved all Privacy Act Statements used when collecting data. See the response to Section 1.1 for a discussion of the manner in which USCIS uses RAPS and APSS data.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

An individual who is the subject of a record in RAPS or APSS may access those records that are not exempt from disclosure. A determination whether a record may be accessed (by the individual or others) will be made at the time a request is received based on FOIA exemptions or Privacy Act exemptions claimed in the SORN.

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to National Records Center, FOIA/PA Office, P.O. Box 648010, Lee's Summit, MO 64064-8010. Specific FOIA contact information can be found at http://www.dhs.gov/foia under "contacts."

When seeking records about yourself from this system of records or any other USCIS system of records, your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, http://www.dhs.gov or 1-866-431-0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you,
- Specify when you believe the records would have been created,
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information, USCIS will not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Individuals have the opportunity to correct inaccurate or erroneous information during a personal interview with a USCIS Asylum Officer.

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

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

Individuals are notified at their interview about the procedures for correcting application information as maintained in RAPS and APSS.

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

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

USCIS provides formal redress for individuals wishing to correct information in RAPS and APSS.

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

Individuals may request access to, or correction of, their personal information pursuant to FOIA and the Privacy Act of 1974.

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

Mitigation: The redress and access measures offered by USCIS are appropriate given the purpose of the system. Individuals are given numerous opportunities during and after the completion of the applications process to correct information they have provided and to respond to information received from other sources. Individuals may avail themselves of the redress and appeal process as stated in the DHS Privacy Act regulations (found at 6 Code of Federal Regulations, Section 5.21).

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

Both government personnel and contractors possessing a mission requirement, have access to RAPS and APSS. Security procedures are in place in accordance with the system security plan and the USCIS systems lifecycle methodology. This plan is the primary reference that documents

system security responsibilities, policies, controls, and procedures. Access to RAPS and APSS is controlled via the DHS PICS Office, which controls user authorizations and authentication controls for all DHS system users.

The DHS Password Issuance and Control System (PICS) Office controls user authorizations and authentication controls for all DHS system users. Officers that have read-only access include adjudications officers who review applications and adjudicate a number of USCIS benefits. All users must access the system formally through terminal emulation software and TCP/IP access, as documented in the system's security documents. (See Section 4 for details on information sharing.) All users have cleared access to system resources granted through the DHS PICS Office.

RAPS and APSS are both legacy INS mainframe systems. Currently, ICE manages the contract for all legacy mainframe systems using the existing DOJ Data Center. This will change over time when DHS establishes its own data center that can house the mainframe systems. DOJ is responsible for the operation and maintenance of the mainframe and applications that run on the mainframe. There is a current Service Level Agreement (SLA) that defines DOJ responsibilities for intrusion detection, physical security, operational security, contingency controls, and reporting of security alerts and incidences. The SLA also defines levels of service to be provided. DHS is responsible for CIS application maintenance, development and testing. These services are performed through government contractors.

The Rules of Behavior for using RAPS and APSS fall under the DHS guidelines for corporate rules of behavior. These rules are clarified and mandated to the user by the DHS guidelines and security documentation. The DHS PICS Office owns copies of these rules. Users agree to abide by these rules when receiving a secured user ID and upon passing a background clearance check.

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

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

Criteria, procedures, controls, and responsibilities regarding RAPS and APSS access are contained in the Sensitive System Security plan for RAPS and APSS. Additionally, there are several department and government-wide regulations and directives that provide additional guidance and direction. Asylum-related data is governed by strict regulatory confidentiality provisions outlined in 8 CFR § 208.6, Disclosure to Third Parties. This regulation generally prohibits the disclosure to third parties of information contained in or pertaining to asylum applications, credible fear

determinations, and reasonable fear determinations -- including information contained in RAPS or APSS, except under certain limited circumstances. Non-asylum users must sign a confidentiality acknowledgement in order to obtain look-only access to RAPS/APSS.

8.2 Will Department contractors have access to the system?

Government contractors have access to RAPS and APSS, perform maintenance software support to correct system problems, and service a Help Desk that provides support Monday through Friday for RAPS- and APSS-related issues. The contract for RAPS and APSS is included in the USCIS Starlight Mainframe Systems Contract. Prior to receiving system access, employees are subject to security background checks, provisions for protecting information, and password issuance. The contractor is required to develop and maintain a comprehensive Computer and Telecommunications Security Program to address the integrity, confidentiality, and availability of sensitive but unclassified (SBU) information during collection, storage, transmission, and disposal. The contractor's security program must adhere to the requirements set forth in DHS security directives and procedures.

Government contractors maintain the RAPS and APSS systems under the direction of the USCIS Office of Information Technology (OIT). Access is provided to contractors only as needed to perform their duties as required in the agreement between USCIS and the contractor and as limited by relevant SOPs. In addition, USCIS employees and contractors who have completed a G-872A & B form (see Section 8.1) and granted appropriate access levels by a supervisor are assigned a login and password to access the system. These users must undergo federally approved clearance investigations and sign appropriate documentation in order to obtain the appropriate access levels.

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

All system users take annual mandatory computer security awareness training. This training includes guidance on federal laws, policies, and regulations relating to privacy and data integrity, as well as the handling of data (including any special restrictions on data use and/or disclosure). The USCIS IT Security Office verifies that training has been successfully completed and maintains a record of certificates of training on all USCIS employees and contractors. Current RAPS and APSS users took the mandatory computer security awareness training in June and July of 2008.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes. The last C&A for these systems was completed in September 2004. USCIS is currently working to renew the Authorization to Operate (ATO).

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

RAPS and APSS are legacy INS mainframe systems that are resident on the DOJ mainframe computer at Justice Data Center – Dallas, Texas. Currently, ICE manages the contract that provides

systems support for the CIS and ICE legacy systems at Dallas. This will change over time when DHS establishes its own data center that can house the mainframe systems. DOJ is responsible for the operation and maintenance of the mainframe and applications that run on the mainframe at the data center because they own the data center. There is a current Service Level Agreement (SLA) that defines DOJ responsibilities for intrusion detection, physical security, operational security, contingency controls, and reporting of security alerts and incidences. The SLA also defines levels of service to be provided. DHS is responsible for RAPS and APSS application maintenance, development, and testing. These services are performed through contractors. The USCIS ISSO works directly with the USCIS OIT, ICE IT, and DOJ to ensure that the SLA is current.

The Rules of Behavior for using RAPS and APSS fall under the DHS guidelines for corporate rules of behavior. These rules are clarified and mandated to the user by the DHS guidelines and security documentation. The DHS PICS Office maintains copies of these rules. Users agree to abide by these rules when receiving a secured user ID and upon passing a background clearance check. In order to reduce the possibility of misuse and inappropriate dissemination of information, DHS security specifications require auditing capabilities that log user activity. All user actions are tracked via audit logs.

Misuse of data in RAPS and APSS is prevented or mitigated by requiring that users conform to appropriate security and privacy policies, follow established rules of behavior, and receive adequate annual security awareness training that addresses their duties and responsibilities to protect the data.

When privileges expire, user access is promptly terminated. After termination of employment at USCIS, access privileges are removed as part of the employee exit clearance process (signed by various persons before departure).

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy Risk: Given the scope of the personal information collected in RAPS and APSS, the security of the information on the system is of critical importance. Due to the sensitive nature of this information, there are inherent security risks (e.g., unauthorized access, use and transmission/sharing) that require mitigation.

Mitigation: To mitigate these risks, a number of business and systems rules have been implemented. Access and security controls have been established to identify and mitigate privacy risks associated with authorized and unauthorized users, namely misuse and inappropriate dissemination of data. Access to the database is given only to users that need it to perform their official duties. All authorized users must authenticate using a user ID and password. Role-based user accounts are used to minimize the number of persons who have access to the system. Audit trails are kept in order to track and identify any unauthorized changes to information in the system. RAPS and APSS have a comprehensive audit trail tracking and maintenance function that stores information on who submits each query, when the query was run, what the response was, who received the response, and when the response was received. Data encryption is employed where appropriate to ensure that only those authorized to view the data may do so and that the data has

not been compromised while in transit. Further, RAPS and APSS comply with DHS and FISMA/NIST security requirements, which provide criteria for securing networks, computers, and computer services against attack and unauthorized information dissemination.

Privacy Risk: Information security.

Mitigation: USCIS has adopted the following information security practices to ensure information security:

USCIS offices are located in buildings with controlled access by security guards or authorized government contractors. Access to government premises is by pre-assigned official identification issued by DHS. Information in this system is also safeguarded in accordance with applicable laws, rules and policies. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards include restricting access to authorized personnel who have a need to know and operating pursuant to the DHS Information Technology Security Programs Handbook, including the use of password protection identification features. RAPS and APSS are maintained at the DOJ Data Center (Dallas). Physical controls of the facility (e.g., guards, locks, etc.) apply and prevent entry by unauthorized entities. RAPS and APSS do not contain classified information.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

RAPS and APSS are case management systems.

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

RAPS and APSS are in the Operation and Maintenance phase of the DHS development system life cycle.

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

RAPS and APSS contain only the information needed to review, interview and fully adjudicate the benefit application that has been filed. Neither RAPS nor APSS has any ability to track, or in any way monitor, the activities or applications of individuals outside of the information required to process the benefit application filed by the applicant.

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security