Privacy Impact Assessment Update
for the

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

DHS/USCIS/PIA-027(b)

June 5, 2013

Contact Point
Donald K. Hawkins
Office of Privacy
United States Citizenship and Immigration Services
(202) 272-8030

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The U.S. Department of Homeland Security (DHS), United States Citizenship and Immigration Services (USCIS) is updating the Privacy Impact Assessment (PIA) for the Refugees, Asylum, and Parole System (RAPS) and the Asylum Pre-Screening System (APSS) in order to provide notice of the expansion in the National Counterterrorism Center (NCTC)'s "temporary retention" of RAPS information due to the March 2012 release of the Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and other Agencies of Information in Datasets Containing Non-Terrorism Information (AG Guidelines).

Introduction

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 Section 208 of the Immigration and Nationality Act (INA), 8 U.S.C. § 1158 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), Pub. L. 105-100, 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.

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.

Pursuant to the National Security Act of 1947, as amended, the National Counterterrorism Center (NCTC) "serve[s] as the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies,

capabilities, and networks of contacts and support" (50 U.S.C. § 404o). In order to enhance information sharing, the President issued Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans (October 27, 2005), which provides that the head of each agency that possesses or acquires terrorism information shall promptly give access to that information to the head of each other agency that has counterterrorism functions. The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 (Pub. L. No. 108-458), as amended, places an obligation on U.S. government agencies to share terrorism information with the Intelligence Community, including NCTC. In certain instances, DHS shares an entire dataset with an Intelligence Community member in order to support the counterterrorism activities of the Intelligence Community and to identify terrorism information within DHS data.

In 2011, DHS began sharing the entire RAPS[1] dataset with NCTC under a Memorandum of Understanding (MOU). In 2013, DHS and NCTC entered into a new Memorandum of Agreement (MOA) that supersedes the 2011 MOU and documents an expansion of routine sharing with NCTC. The MOA permits NCTC to use RAPS information to facilitate NCTC's counterterrorism efforts and helps to ensure that immigration benefits are not granted to individuals who pose a threat to national security. This information sharing also aligns with DHS's mission to prevent and deter terrorist attacks. Pursuant to 8 CFR § 208.6(a), the Secretary has authorized regular sharing of asylum-related information for this purpose. The MOA includes a number of safeguards to ensure the information is only used for the purposes explicitly permitted under the MOA, this PIA, and the DHS/USCIS-010 Asylum Information and Pre-Screening SORN (January 5, 2010, 75 FR 409). The MOA also limits the amount of time the information is maintained at NCTC, ensures proper information technology security is in place during and after transmission of the RAPS information to NCTC, requires training on interpreting RAPS information, and provides for routine reporting and auditing of NCTC's use of the information.

Reason for the PIA Update

USCIS is updating the existing PIA (DHS/USCIS/PIA-027)[2], to provide notice of an expansion in NCTC's 'temporary retention' of RAPS information.[3] Under Executive Order 12333, United States Intelligence Activities (December 8, 1981), as amended, IC elements are required to have guidelines approved by the Attorney General of the United States for the collection, retention, and dissemination of information concerning United States Persons (U.S.

[1] The MOA does not include the APSS database.
[2] The existing DHS/USCIS/PIA-027 was first published on November 24, 2009, and updated subsequently on June 30, 2011.
[3] The purpose of this temporary retention period is to allow NCTC sufficient time to determine whether the U.S. Person information it receives from other federal departments and agencies is terrorism information.

Persons).[4] These guidelines outline temporary retention periods during which an IC element must determine whether it can continue to retain U.S. Person information, consistent with Executive Order 12333 and the purposes and procedures outlined in its guidelines.

In March 2012, the Attorney General of the United States approved Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and other Agencies of Information in Data Sets Containing Non-Terrorism Information (AG Guidelines).[5] These Guidelines establish an outside limit of five years for NCTC's temporary retention of U.S. Person information obtained from the datasets[6] of other federal departments and agencies. The purpose of this temporary retention is to provide NCTC sufficient time to determine whether the U.S. Person information it receives from other federal departments and agencies is terrorism information.[7] The AG Guidelines allow NCTC to retain all information in the datasets it receives for the full temporary retention period,[8] whereby the information may be "continually assessed" against new intelligence to identify previously unknown links to terrorism.[9] NCTC may only retain U.S. Person information within such datasets beyond the temporary retention period if the information is "reasonably believed to constitute terrorism information."[10] In light of the new AG Guidelines, NCTC requested that DHS re-evaluate its information sharing and access agreements with NCTC, including the 2011 MOU to share RAPS information.

---

[4] NCTC's Guidelines use the definition of U.S. Person provided in Executive Order 12333, which states that a U.S. Person is "a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments." See Executive Order 12333, Section 3.5(k).

[5] See NCTC's AG Guidelines, available at http://www.nctc.gov/docs/NCTC Guidelines.pdf.

[6] In the context of DHS's information sharing relationship with NCTC, a "dataset" refers to a collection of information about a set of individuals that DHS has gathered during its routine interactions (e.g., screening travelers, reviewing immigration benefit applications, issuing immigration benefits) with the public. Consequently, DHS datasets contain information about individuals who have no connection to terrorism. A dataset may constitute all the records in a Privacy Act System of Records, or a portion of the records therein.

[7] NCTC's AG Guidelines use the statutory definition of "terrorism information" in Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, which states "the term 'terrorism information'—(A) means 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(a)(5).

[8] As noted later in the PIA, the Guidelines allow departments and agencies to negotiate the terms and conditions of information sharing and access agreements. Through these negotiations, departments and agencies may establish temporary retentions period that are less than the five year outside limit established by the AG Guidelines. DHS's agreement with NCTC for RAPS information establishes a temporary retention period of three years for reasons explained later in the PIA.

[9] See NCTC's AG Guidelines, available at http://www.nctc.gov/docs/NCTC Guidelines.pdf.

[10] See NCTC's AG Guidelines, available at http://www.nctc.gov/docs/NCTC Guidelines.pdf.

The AG Guidelines preserve the Department's authority to negotiate with NCTC the terms and conditions of information sharing and access agreements relating to, among other things, "privacy or civil rights or civil liberties concerns and protections."[11] One such protection is the amount of time NCTC may retain DHS data that does not constitute terrorism information. With this in mind, DHS developed a Data Retention Framework of Factors to determine appropriate temporary retention periods for DHS datasets on a system-by-system basis. This Framework includes factors related to the sensitivity of a dataset and operational considerations. Factors related to the sensitivity of a dataset include: the circumstances of collection, the amount of U.S. Person information in the dataset, and the sensitivity of the particular data fields (e.g., sensitive personally identifiable information) that are requested. Operational factors include: the mission benefits to DHS, the mission benefits to NCTC, and any limitations for the DHS data steward (e.g., DHS's own retention period for the dataset). Using the Data Retention Framework of Factors, DHS and NCTC agreed to a three year temporary retention period for all RAPS information provided to NCTC.

RAPS information is further controlled by regulations related to asylum information. The federal regulation at 8 CFR § 208.6 generally prohibits the disclosure to third parties of information contained in or pertaining to asylum applications—including information contained in RAPS—except under certain limited circumstances. Pursuant to 8 CFR § 208.6(a), the Secretary of Homeland Security may specifically authorize the disclosure of asylum-related information, and the Secretary has authorized DHS to share asylum-related information with elements of the Intelligence Community and agencies with counterterrorism functions. These organizations may retain asylum-related information for a maximum period of three years, unless the asylum-related information is identified as terrorism information or, in the case of an Intelligence Community element, as information determined to be relevant to the element's authorized intelligence function(s).

The 2013 MOA documents NCTC's expanded temporary retention period and augments the privacy protections of the 2011 agreement with NCTC. The MOA continues to recognize the special considerations attendant with using, retaining, and dissemination RAPS information. In addition, the MOA augments privacy protections related to transparency, redress, and oversight. To promote transparency, the MOA requires DHS and NCTC to develop public PIAs that provide notice regarding the existence and contents of the MOA and to cooperate to promote transparency through efforts such as joint presentations to Congress and the DHS Data Privacy and Integrity Advisory Committee. With respect to redress, the MOA requires NCTC to establish a redress mechanism for individuals whose PII has been retained as terrorism information. The redress process will direct any request for correction or redress to DHS for resolution, as appropriate. For any records corrected by DHS through this process, NCTC will

[11] See NCTC's AG Guidelines, available at http://www.nctc.gov/docs/NCTC Guidelines.pdf.

correct those records in its possession when it receives a notification of the correction from DHS. To increase oversight, DHS and NCTC have refined the quarterly reporting requirements regarding NCTC's use and retention of the DHS information. Additionally, the MOA allows DHS to assign an on-site oversight representative to NCTC to provide intelligence, data stewardship, privacy, civil rights, and civil liberties oversight of the handling of DHS information by NCTC.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

There is no change in the collection of RAPS and APSS information.

Uses of the System and the Information

There are no changes to the uses of the system and the information described in the RAPS and APSS PIA.

Retention

The DHS retention period for RAPS and APSS have not changed.

Pursuant to the MOA, NCTC will now be allowed to temporarily retain RAPS information for up to three years in order to identify terrorism information, in support of its counterterrorism mission and in support of DHS's mission. NCTC previously retained RAPS information for 180 days. The three year temporary retention period commences when DHS delivers the RAPS information to NCTC. When NCTC replicates RAPS information, the records will be marked with a "time-to-live" date, which will specify when the RAPS information will be deleted if it is not identified as terrorism information. NCTC will purge all RAPS records not determined to constitute terrorism information no later than three years from receipt of the record from DHS. This process will be audited as required under the MOA.

Since NCTC's AG Guidelines allow information to be "continually assessed" during the temporary retention period,[12] NCTC may retain all RAPS information for three years, regardless of whether NCTC has made a terrorism information determination about a particular RAPS record, as it is possible that new intelligence or terrorism information will identify previously unknown terrorism information within that RAPS record. NCTC may retain RAPS records determined to constitute terrorism information in accordance with NCTC's authorities and policies, applicable law, and the terms of the MOA.

[12] See NCTC's AG Guidelines, available at http://www.nctc.gov/docs/NCTC Guidelines.pdf.

Internal Sharing and Disclosure

There are no changes to the internal sharing and disclosures described in the RAPS and APSS PIA.

External Sharing and Disclosure

DHS has entered into an updated MOA with NCTC in order to facilitate NCTC's counterterrorism efforts and to identify terrorism information within RAPS. Pursuant to 8 CFR § 208.6(a), the Secretary has authorized regular sharing of asylum-related information for this purpose. This information sharing also aligns with DHS's mission to prevent and deter terrorist attacks and helps to ensure that immigration benefits are not granted to individuals who pose a threat to national security. This sharing is conducted pursuant to routine uses H and I of the DHS/USCIS-010 SORN, which states that DHS may share RAPS and APSS information with "any element of the U.S. Intelligence Community, or any other federal or state agency having a counterterrorism function, provided that the need to examine the information or the request is made in connection with its authorized intelligence or counterterrorism function or functions and the information received will be used for the authorized purpose for which it is requested."

A material condition for DHS's sharing RAPS information with NCTC is that the sharing must provide real and ongoing value to both NCTC's and DHS's missions. NCTC replicates RAPS information into its Counterterrorism Data Layer (CTDL) to support its counterterrorism efforts. The CTDL provides NCTC analysts "with the ability to search, exploit, and correlate terrorism information in a single environment."[13] For example, NCTC analysts may run queries against RAPS information in the CTDL to identify terrorism information within RAPS. When RAPS information is determined to constitute terrorism information, NCTC will provide feedback to DHS, which DHS may use to support its mission to prevent and deter terrorist attacks.

Additionally, NCTC will conduct automated screening of all RAPS information to generate potential leads that may constitute terrorism information. NCTC analysts will review all of the potential leads to determine whether the RAPS information constitutes terrorism information. NCTC will process all RAPS records through this screening support process within the temporary retention period of three years to determine whether RAPS records constitute terrorism information. This screening support activity supports DHS's mission to prevent and deter terrorist attacks and assists DHS in its assessment of the national security risk that may be posed by granting asylum status to applicants. Because this screening support assists DHS, the MOA includes provisions to allow DHS, in coordination with NCTC, to perform the review of

[13] See "Information Sharing Environment Annual Report to the Congress: National Security Through Responsible Information Sharing," dated June 30, 2012. Available at: http:// http://ise.gov/sites/default/files/ISE_Annual_Report_to_Congress_2012.pdf.

the automated matches if NCTC resources or workload prioritization preclude NCTC from providing this review.

NCTC will review, retain, and disseminate RAPS records it has determined to constitute terrorism information in accordance with procedures approved for NCTC by the Attorney General in accordance with Section 2.3 of Executive Order 12333, and additional terms specified in the MOA.

The MOA has strict safeguards to protect the PII provided to NCTC. These protections include limitations on disclosures to foreign governments. In addition, the completion of training on privacy and RAPS information is a requirement for NCTC personnel to receive and maintain access to RAPS. The agreement stipulates that both DHS and NCTC personnel will be appropriately trained regarding the proper treatment of PII and proper care of the information systems used to ensure the overall safeguarding of the information in addition to applicable rules and conditions concerning United States Persons information. DHS and NCTC will each ensure that its employees, including contractors with access to any of the other Party's records, have completed privacy training on the handling of PII.

Within 30 days of signing the new MOA, DHS/USCIS will provide initial training to all current NCTC users of RAPS information on RAPS, protections for asylum and refugee-related information, and other Special Protected Classes of individuals as they relate to RAPS information. New NCTC users of RAPS information will complete the appropriate initial training before they access RAPS information. All NCTC users who access RAPS information will complete refresher training provided by DHS/USCIS at least annually in order to retain their access. Additionally, the MOA allows DHS to assign an on-site oversight representative to NCTC to provide intelligence, data stewardship, privacy, civil rights, and civil liberties oversight of the handling of DHS information by NCTC.

The MOA stipulates that NCTC may not disseminate to third parties information derived from RAPS information unless that information is identified as terrorism information. The MOA also establishes procedures for NCTC's dissemination of RAPS information that has been identified as terrorism information. NCTC will maintain an electronic copy of the RAPS information that is disseminated, including to whom the information is disseminated and the purpose for the dissemination. However, if there is a question on RAPS information and its relationship to terrorism, NCTC may request permission from DHS to share this RAPS information with other intelligence agencies.

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

Notice

The system of records notice for RAPS and APSS was published on January 5, 2010, 75 FR 409, and remains accurate and current. Routine uses H and I cover this sharing.

Individual Access, Redress, and Correction

There are no changes to the access, redress, and correction procedures described in the RAPS and APSS PIA.

Technical Access and Security

No changes.

Technology

No changes.

Responsible Official

Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
U.S. Department of Homeland Security

Approval Signature

Original signed copy on file with DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Privacy Impact Assessment
for the

USCIS Asylum Division

DHS/USCIS/PIA-027(c)

July 21, 2017

Contact Point
Donald K. Hawkins
Privacy Officers
U.S. Citizenship and Immigration Services
(202) 272-8000

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Asylum Division of the U.S. Citizenship and Immigration Services (USCIS) adjudicates applications for asylum, benefits pursuant to Section 203 of the Nicaraguan Adjustment and Central American Relief Act (NACARA § 203), withholding of removal under the terms of a settlement agreement reached in a class action[1], and screening determinations for safe third country, credible fear, and reasonable fear. The Asylum Division 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), are used by the USCIS Asylum Division[2] 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).[3] USCIS is updating and reissuing this Privacy Impact Assessment (PIA) because the Asylum Division manages records and systems containing personally identifiable information (PII) in order to conduct its adjudications.

Overview

U.S. Citizenship and Immigration Services (USCIS) is the component of the Department of Homeland Security (DHS) that oversees lawful immigration to the United States. As set forth in Section 451(b) of the Homeland Security Act of 2002, Public Law 107-296, Congress charged USCIS with administering the asylum program. USCIS, through its Asylum Division, administers the affirmative asylum program to provide 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 Section 208 of the Immigration and Nationality Act (INA), 8 U.S.C. § 1158 and 8 CFR § 208. The USCIS Asylum Division also adjudicates the benefit program established by the Nicaraguan Adjustment and Central American Relief Act (NACARA) § 203 and administers safe third country, credible fear, and reasonable fear screening processes.[4] This Privacy Impact Assessment examines the USCIS Asylum Division program, the information that it collects, as well as its case management systems and support information technology systems.

The Asylum Division supports the following four programs:

[1] American Baptist Churches v. Thornburgh, 760 F. Supp. 796 (N.D. Cal. 1991) (ABC Settlement).
[2] 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, they were never included operationally.
[3] Pub. L. No. 105-100, 111 Stat. 2193 (1997), amended by Pub. L. No. 105-139, 111 Stat. 2644 (December 2, 1997).
[4] Section 203 of Pub. L. No. 105-100.

1) Affirmative Asylum[5]

Foreign nationals may seek protection through asylum if they suffered persecution or fear that they will suffer persecution on account of race, religion, nationality, membership in a particular social group, or political opinion. To obtain asylum, the individual must be physically present in the United States. There are two ways to apply for asylum in the United States: through the affirmative asylum process and the defensive asylum process.

The Asylum Division is responsible for the administration of the affirmative asylum process and adjudication of the affirmative asylum application. An individual not in removal proceedings may apply for asylum through the affirmative asylum process regardless of how he or she arrived in the United States or his or her current immigration status by filing Form I-589, Application for Asylum and for Withholding of Removal,[6] with USCIS. An individual may also file Form I-589 as a defensive application in removal proceedings before an Immigration Judge of the Department of Justice's (DOJ) Executive Office for Immigration Review (EOIR).[7]

An asylum applicant may include in the application his or her spouse and any children as dependent asylum applicants if they are in the United States, comply with the requirements of providing biometrics, and appear at the asylum interview.[8] A grant of asylum to the principal asylum applicant is the basis for a grant of asylum to the spouse and any children included as dependent applicants as long as the spouse or child is in the United States and not otherwise barred from a grant of asylum. Additionally, Form I-589 requests information on each applicant's parents, siblings, former spouses, and children, regardless of whether they are included as dependent applicants.

2) Nicaraguan Adjustment and Central American Relief Act (NACARA Section 203)[9]

NACARA § 203 allows individuals who meet certain criteria, along with qualifying family members, to apply for suspension of deportation or for special rule cancellation of removal under

[5] See INA § 208; see also 8 CFR § 208, describing the asylum process.
[6] Witholding of Removal must be granted when the evidence establishes that it is more likely than not that the applicant's life or freedom is threatened of account of race, religion, nationality, membership in a particular social group, or political opinion in the proposed country of removal.
[7] Immigration Judges are adjudicators within the Department of Justice's Executive Office for Immigration Review (EOIR). Persons whose removal is being sought by DHS generally appear before an Immigration Judge who will adjudicate any benefit or protection for which the foreign national may be eligible, including asylum and withholding of removal.
[8] Children under the age of 14 are not required to provide a signature on an application, petition, or request filed with USCIS, but they may choose to sign their name during their ASC appointment if they are capable of signing. A parent or legal guardian may also sign the application, petition, or request on the child's behalf.
[9] NACARA § 203 applies to certain individuals from Guatemala, El Salvador, and the former Soviet bloc countries (the Soviet Union or any republic of the former Soviet Union, such as Russia, Latvia, Lithuania, Estonia, Albania, Bulgaria, the former Czechoslovakia, the former East Germany, Hungary, Poland, Romania, or Yugoslavia or any state of the former Yugoslavia) who entered the United States and applied for asylum by specified dates or registered for benefits as well as certain of their relatives. See 8 CFR §§ 240.60 - 204.70.

the standards for suspension of deportation similar to those in effect before the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA).[10] Form I-881, Application for Suspension of Deportation or Special Rule Cancellation of Removal is used to apply for benefits under NACARA § 203.

Form I-881 solicits biographic information about the applicant; their presence in the United States; entries and departures; the applicant's financial status and employment; information about the applicant's current spouse, former spouses, children, and parents; information relating to the eligibility criteria for benefits under NACARA § 203;[11] and information about the Form I-881 preparer, if prepared by someone other than the applicant. Applicants must also comply with the requirements of providing biometrics.

3) Credible Fear Screenings[12]

Individuals subject to expedited removal who indicate an intention to apply for asylum, express a fear of persecution or torture, or a fear of return to their home country are referred to USCIS Asylum Officers to determine whether they have a credible fear of persecution or torture. Individuals found to have a credible fear of persecution or torture are placed in removal proceedings under INA § 240 and may apply for asylum or withholding of removal as a defense to removal before an Immigration Judge by filing Form I-589, or pursue other forms of relief or protection from removal. The Asylum Division electronically receives information about credible fear applicants through referral documentation provided by U.S. Immigration and Customs Enforcement (ICE) or U.S. Customs and Border Protection (CBP). The referral documentation includes forms containing information about the applicant: Form I-860, Notice and Order of Expedited Removal, and Form I-867, A&B, Record of Statement in Proceedings under Section 235(b)(1) of the Act & Jurat for Record of Sworn Statement in Proceedings under Section 235(b)(1) of the Act.

As part of the credible fear screening adjudication, Asylum Officers prepare Form I-870, Record of Determination/Credible Fear Worksheet. This worksheet includes biographic information about the applicant, including the applicant's name, date of birth, gender, country of

[10] See Pub. L. 104-208.

[11] Form I-881 solicits information used to determine whether the applicant can demonstrate good moral character for the seven years prior to filing the application, and whether the applicant or his or her United States Citizen or lawful permanent resident spouse, parent, or child will suffer extreme hardship if the applicant is removed from the United States. See 8 CFR §§ 240.60 - 240.70.

[12] Section 235 of the INA, as amended, and its implementing regulations provide that certain categories of individuals are subject to expedited removal without a hearing before an Immigration Judge. These include: arriving stowaways; certain arriving aliens at ports of entry who are inadmissible under section 212(a)(6)(C) of the INA (because they have presented fraudulent documents or made a false claim to U.S. citizenship or other material misrepresentations to gain admission or other immigration benefits) or 212(a)(7) of the INA (because they lack proper documents to gain admission); and certain designated aliens who have not been admitted or paroled into the United States and who are inadmissible under INA 212(a)(6)(C) or (7). See also 8 C.F.R. § 235.3 and 8 C.F.R. § 208.30.

birth, nationality, ethnicity, religion, language, and information about the applicant's entry into the United States and place of detention. Additionally, Form I-870 collects sufficient information about the applicant's marital status, spouse, and children to determine whether they may be included in the determination. Form I-870 also documents the interpreter ID number of the interpreter used during the credible fear interview and collects information about a relative or sponsor in the United States, including their relationship to the applicant and contact information.

4) Reasonable Fear Screenings[13]

Sections 238(b) and 241(a)(5) of the INA provide for streamlined removal procedures that prohibit certain individuals subject to a final administrative removal order under section 238(b) or whose prior order of exclusion, deportation, or removal is reinstated under section 241(a)(5) of the INA, from contesting removability before an Immigration Judge and from seeking any relief from removal. If an individual ordered removed under either section 238(b) or section 241(a)(5) of the INA expresses a fear of return to the country to which he or she has been ordered removed, the case must be referred to a USCIS Asylum Officer to determine whether the individual has a reasonable fear of persecution or torture. Individuals found to have a reasonable fear of persecution or torture are referred to an Immigration Judge for withholding-only proceedings in which they may seek withholding of removal under INA § 241(b)(3), or withholding or deferral of removal under regulations implementing U.S. obligations under the Convention Against Torture by filing Form I-589. The referral documentation that USCIS receives from ICE with information about the applicant includes either a fully executed Form I-851A, Final Administrative Removal Order; or a fully executed Form I-871, Notice of Intent/Decision to Reinstate Prior Order and a copy of the prior order of removal.

As part of the reasonable fear screening process, USCIS Asylum Officers prepare Form I-899, Record of Determination/Reasonable Fear Worksheet. This worksheet includes biographic information about the applicant, including the applicant's name, date of birth, gender, country of birth, nationality, ethnicity, religion, language, and information about the applicant's entry into the United States and place of detention. Form I-899 also documents the interpreter ID number of the interpreter used during the reasonable fear interview.

Information Technology (IT) and Support Systems

The USCIS Asylum Division is primarily served by two information technology data systems:

1) Refugees, Asylum, and Parole System (RAPS) is a comprehensive case management tool that enables USCIS to handle and process applications for asylum pursuant to Section 208

[13] See 8 C.F.R. §§ 238.1, 241.8, 208.31.

of the INA and applications for suspension of deportation or special rule cancellation of removal pursuant to NACARA § 203.

Private Attorney Maintenance System (PAMS) is a subsystem RAPS. It maintains data on applicants' attorneys such as name, firm, and address. Each attorney is identified by an identification code, consisting of the office code and a sequential number. PAMS links to RAPS and stores attorney's address information.

2) Asylum Pre-Screening System (APSS) is a case management system that supports USCIS in the screening of individuals in the credible fear and reasonable fear processes.

These systems are used to capture information pertaining to asylum applications, credible fear and reasonable fear screening processes, and applications for benefits provided by NACARA § 203.

The USCIS Asylum Division uses RAPS and APSS to track case status and facilitate the scheduling of appointments and interviews, and the issuance of notices (including receipt notices, interview appointment notices, and decision letters) at several stages of the adjudication process. 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 a means for analyzing and managing program workflows and provide the Asylum Program with statistical reports to assist with oversight of production and processing goals.

In addition to RAPS and APSS, the USCIS Asylum Division also uses SharePoint,[14] referred to as Enterprise Collaboration Network (ECN),[15] and locally-developed applications (LDA)[16] to support its mission and day-to-day functions. Asylum Division information may be hosted on internal ECN networks and LDAs. The Asylum Division ECN site and LDAs provide a secure environment to facilitate collaboration among Asylum Division personnel across its field offices and headquarters. The appendices to this PIA delineate USCIS Asylum Division's use of ECN and LDAs for the processing of asylum applications, NACARA § 203 applications, and credible fear and reasonable fear screenings. RAPS or APSS information, including Sensitive PII, that may otherwise have been stored on a shared drive or transmitted via email may be hosted on internal SharePoint/ECN networks in order to reduce dependency on those tools and minimize associated costs and technical limitations.

[14] SharePoint is a commercial off-the-shelf (COTS) web-based application that provides a platform on which to build custom applications and features a suite of collaboration, document management, and communication tools, as well as a high degree of integration with other Microsoft Office products.
[15] The Asylum Division SharePoint environment provides offices the ability to quickly and electronically meet their business needs through the use of document, workflow, form, and records management as well as reporting, auditing, and organizational capabilities.
[16] A LDA is an application that stores, processes, or transmits USCIS data, but is not currently recognized as an official USCIS system within the USCIS IT inventory, and has not been brought into FISMA compliance to meet DHS IT Security policies.

The Asylum Division's use of SharePoint/ECN is consistent with the Privacy Impact Assessment for DHS Employee Collaboration Tools.[17] The Asylum Division SharePoint/ECN site collection provides a secure environment to facilitate collaboration among Asylum Division personnel across its field offices and headquarters. Information in the SharePoint/ECN site collection is protected using security safeguards established by DHS. Asylum Division SharePoint sites have designated facilitators responsible for determining user access and ensuring that the sites are only used for approved purposes, such as internal collaboration, document hosting, and workflow management. These facilitators receive special training and actively manage permissions to ensure that only users with a need-to-know have access to information on the Asylum SharePoint/ECN sites. The Asylum Division SharePoint site collection designates pages approved to host sensitive PII with a "Sensitive Personally Identifiable Information Allowed" banner at the top of each page.

Refugee, Asylum, and Parole System (RAPS)

RAPS is a comprehensive case management tool that enables USCIS to handle and process applications for asylum and applications for suspension of deportation or special rule cancellation of removal pursuant to NACARA § 203. USCIS, ICE, and CBP offices worldwide can access RAPS data through the Person Centric Query System (PCQS) as a resource of current and historic immigration status information on more than one million applicants.[18] DHS officials can use RAPS to verify the status of asylum applicants, asylees (individuals granted asylum), and their derivatives 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.

Preliminary Processing of Application:

As described in the Benefit Request Intake Process PIA,[19] an asylum or NACARA § 203 accredited representative[20] or legal representative[21] (hereafter collectively referred to as legal representative) submits an application and supporting documentation to USCIS. Asylum applicants file 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. NACARA § 203 applicants file Form I-881, The Application for Suspension of Deportation or Special Rule Cancellation of Removal. Service Center or Asylum personnel receive the application by mail and manually enter most of the information from a new application into RAPS.

---

[17] See DHS/ALL/PIA-059 Employee Collaboration Tools, available at www.dhs.gov/privacy.
[18] See DHS/USCIS/PIA-010 Person Centric Query Service, available at www.dhs.gov/privacy.
[19] See DHS/USCIS/PIA-061 Benefit Request Intake Process, available at www.dhs.gov/privacy.
[20] A person who is approved by the Board of Immigration Appeals (the Board or BIA) to represent aliens before the Immigration Courts and USCIS. The organization must be authorized by the Board to represent aliens.
[21] An attorney or a BIA-accredited representative can represent a benefit requestor before USCIS, as a legal representative with an approved G-28, Notice of Entry of Appearance as Attorney or Accredited Representative on file.

The Form I-589 and Form I-881 collect biographic and demographic information about the applicant, including the applicant's full name, Alien Number (A-Number), Social Security number (SSN), gender, marital status, religious affiliations, nationality, ethnicity, race, hair and eye color, and weight, as well as travel, educational, residential, and employment history. Similar biographic information is collected for any dependent spouse or children who are included on the application. These applications allow the applicant to present details of his or her substantive claim for the requested benefit and to supplement his or her application with additional documentary evidence relevant to his or her claim.

Rather than redundantly storing data on attorneys representing asylum applicants, RAPS links to the Private Attorney Maintenance System (PAMS) and stores only the attorney ID, a value that uniquely identifies the attorney. PAMS contains data on benefit requestor's attorneys such as name, firm, and address. Each attorney is identified by an identification code, consisting of the office code and a sequential number. USCIS uses the attorney ID in RAPS to retrieve attorney data from PAMS, such as name and contact information, for purposes of display in RAPS and for creating attorney copies of all correspondence with the applicant.

When a new case is created in RAPS, the system electronically sends A-Numbers to the Central Index System (CIS) to either create a record or update an existing record.[22] The purpose of CIS is to provide a searchable central index of A-Files as needed in support of immigration benefit and enforcement actions. CIS returns records associated with an A-Number used to ascertain an individual's current and prior immigration status.

RAPS also interfaces with the National File Tracking System (NFTS), which is an automated file-tracking system used to maintain an accurate file inventory and track the physical location of A-Files,[23] to share file location information, and to electronically input the A-Number and File Control Office (FCO) into NFTS.[24] When a user requires the A-File, the user goes to CIS and requests the file. CIS has a direct interface with NFTS to request the file. NFTS maintains and controls the inventory of all A-Files, queries the file location, and manages the request and transfer of A-Files between Asylum Offices and FCOs.

Background, Identity, and Security Checks

Asylum and NACARA § 203 applicants are subject to background, identity, and security 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, identity, and security checks as part of regular case processing.

[22] See DHS/USCIS/PIA-009 Central Index System (CIS), available at www.dhs.gov/privacy.
[23] NFTS does not store a digitized copy or the entire content of the immigration files.
[24] See DHS/USCIS/PIA-032 National File Tracking System (NFTS), available at www.dhs.gov/privacy.

Once the information in the I-589 is entered into RAPS, USCIS generates an appointment notice for the collection of biometrics. The Asylum Division uses the National Appointment Scheduling System (NASS) to schedule appointments for fingerprinting at a USCIS Application Support Center (ASC). USCIS personnel may schedule NASS appointments automatically or manually.[25] NASS may automatically generate appointments through an interface with RAPS. USCIS personnel may manually expedite such a process by requesting an appointment for certain benefit requestors directly in NASS.

Applicants are required to appear at an ASC to be fingerprinted and have their photograph taken. USCIS electronically captures the applicant's fingerprints, photograph, and related biographic data required to verify the individual's identity and to ensure that the correct biographic information is associated with the captured biometrics. Biometric data is captured in Customer Profile Management System (CPMS), which is the centralized source of biometric images used for USCIS benefit card and document production.[26] Biometric and biographic data are also sent to the print production systems for employment authorization documents. Once biometrics are collected, they are submitted for enrollment in DHS's Automated Biometric Identification System (IDENT)[27] for vetting against the Department of Defense (DoD) Automated Biometric Information System (ABIS),[28] and to the Federal Bureau of Investigation (FBI) for vetting against the Next Generation Information (NGI) system.[29] The results from CPMS are uploaded into RAPS.

RAPS also automatically initiates several background, identity, and security checks, querying records held by DHS (e.g., ICE ENFORCE Alien Removal Module (EARM)), the FBI (including FBI name check[30]) and the National Counterterrorism Center (NCTC). RAPS receives and stores the results of these automatically initiated checks. In addition to automatically initiated checks, asylum data may be used for additional background, identity, and security checks during the process of vetting a case for adjudication. These may include the use of classified systems, social media checks, analysis by the CBP National Targeting Center, or other forms of analysis and verification, the results of which may be stored in RAPS or APSS.

Results of Background and Security Checks

Results of background and security check systems are stored in RAPS. Depending on the system, checks are based on biographic search parameters (e.g. name and date of birth) or

[25] See DHS/USCIS/PIA-057 National Appointment Scheduling Systems (NASS) available at www.dhs.gov/privacy.
[26] See DHS/USCIS/PIA-060 Customer Profile Management Service (CPMS), available at www.dhs.gov/privacy.
[27] See DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), available at www.dhs.gov/privacy.
[28] Department of Defense Detainee Biometric Information System, 72 FR 14534 (Mar. 28, 2007).
[29] See Privacy Impact Assessment Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Biometric Interoperability for more information, available at https://www.fbi.gov/foia/privacy-impact-assessments/iafis-ngiinteroperability-1.
[30] See DOJ/FBI-002 Central Records System (CRS), 66 FR 29994 (June 4, 2001).

biometric search parameters. Results are added to RAPS for newly filed applications and can be updated whenever a check is reinitiated to renew an expiring check or prior to a decision. Each check and law enforcement system is briefly summarized below.

- CBP TECS[31] performs a check on the individual's name and date of birth and returns a positive or negative response to RAPS or APSS.
- ICE ENFORCE Alien Removal Module (EARM)[32] performs a check on the individual's A-Number and returns a positive or negative response to RAPS.
- Federal Bureau of Investigation (FBI) Fingerprint Check,[33] through Next Generation Identification (NGI), performs recurring biometric record checks pertaining to criminal history and immigration data. A check on the individual's biometrics returns the date of the applicant's biometrics appointment at a USCIS Application Support Center (ASC), the date the biometrics were sent to the FBI, and the date and result of the check. All FBI fingerprint check requests and responses are routed to NGI via the USCIS Enterprise Service Bus (ESB) and IDENT. There is no direct connection between the FBI's NGI and CPMS.[34]
- FBI Name Check[35] inspects all names and dates of birth used by the individual that are entered into RAPS or APSS and submits them via RAPS or APSS to the FBI. The FBI Name Check response is stored in RAPS or APSS.
- DHS Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT)[36] provides a biometric record check related to travel and immigration history for individuals, including immigration violations, and law enforcement and national security concerns. A check on the individual's biometrics returns the individual's encounter identification number assigned by Office of Biometric Identity Management (OBIM)/IDENT, the dates that the information is collected and uploaded to the system, and the nature of the record into RAPS.
- Department of Defense (DoD) Automated Biometric Identification System (ABIS)[37] is a biometric record check of DoD holdings.[38] A check on the individual's biometrics

[31] See DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS), available at www.dhs.gov/privacy.
[32] See DHS/ICE-PIA-015 ENFORCE Alien Removal Module (EARM), available at www.dhs.gov/privacy.
[33] The FBI replaced its Integrated Automated Fingerprint Identification System (IAFIS) with the Next Generation Identification (NGI). Please see the Privacy Impact Assessment Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Biometric Interoperability for more information, available at https://www.fbi.gov/foia/privacy-impact-assessments/iafis-ngi-interoperability-1.
[34] See DHS/NPPD/PIA-060 CPMS, available at www.dhs.gov/privacy.
[35] See DOJ/FBI-002 Central Records System (CRS), 66 FR 29994 (June 4, 2001).
[36] See DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), available at www.dhs.gov/privacy.
[37] Department of Defense Detainee Biometric Information System, 72 FR 14534 (Mar. 28, 2007).
[38] Biometric data is collected at an authorized biometric capture site, including USCIS offices, Application Support

returns the individual's DoD ABIS vetting result and result date into RAPS. All DoD fingerprint check requests and responses currently flow through CPMS via ESB. There is no direct connection between ABIS and CPMS. CPMS generates a daily report of DoD ABIS vetting results for applicants vetted that day, and this data is entered into RAPS.

- National Counter Terrorism Center (NCTC) performs a check on the individual's biographic information contained in RAPS that is submitted to the NCTC. Results are transmitted through secure means. Results are not currently stored in RAPS, but the checks are done using information extracted from RAPS.

Background, identity, 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.

Interview

In order to adjudicate applications for immigration benefits and protection screenings, Asylum Officers interview applicants. Asylum Officers advise applicants of their legal and procedural protections and receive specialized training on eliciting testimony through non-adversarial interviews. Asylum Officers take notes during the interview, which are included in the applicant's A-File and serves as a reference for drafting the Asylum Officer's assessment or decision worksheet. The Asylum Officer may also elicit information about the applicant's attorney or interpreter during the interview. A contracted interpreter monitor may be present telephonically to ensure the accuracy of the interpretation.

The applicant is required to appear for an interview at a domestic Asylum Office or asylum interview location. RAPS is used to schedule interview appointments, to track the date and status of interview appointments, and to generate interview notices. The USCIS Enterprise Print Management System (EPMS) may be used to generate notices in the future. USCIS Asylum Offices mail the Interview Notice to the applicant and, if applicable, his or her legal representative. Interview information is also added to the A-File, as required by case adjudication Standard Operating Procedures (SOP).

All individuals who arrive at a USCIS Asylum Office for an interview are biometrically verified using the CPMS Identity Verification Tool (IVT).[39] IVT allows USCIS Asylum Offices to compare an individual's biometric (fingerprint and photograph) and biographic information to information previously captured at an ASC, ensuring that the person who appeared at the ASC is

Centers, or U.S. consular offices and military installations abroad using USCIS LiveScan. See the DHS/USCIS/PIA-060 CPMS for more information available at www.dhs.gov/privacy.

[39] See DHS/USCIS/PIA-060 Customer Profile Management System, available at www.dhs.gov/privacy.

the same person appearing at the USCIS Asylum Office.

Decision

After conducting background, identity, and security checks, a substantive interview on the applicant's credibility, merits of the claim, and any potential mandatory bars, and reviewing the record, USCIS Asylum Officers make a determination on the benefit request. USCIS personnel may grant, deny, or revoke an immigration benefit. USCIS personnel may also allow the applicant or beneficiary to withdraw his or her application for the benefit. In certain circumstances, a benefit application may also be administratively closed. USCIS personnel also refer an asylum applicant who is out of status to the Immigration Court for removal proceedings under INA § 240 if the applicant is not found eligible for asylum or NACARA § 203. USCIS records and tracks case decision actions in RAPS. Following adjudication, RAPS sends a daily file to Computer Linked Application Information Management System (CLAIMS 3)[40] with records on individuals for all granted asylum applications who are eligible to receive a secure employment authorization document (EAD). CLAIMS 3 processes the RAPS-generated request. This process is further detailed in the forthcoming USCIS Benefit Decision and Output PIA.[41]

Employment Authorization

Applicants with a pending asylum application can apply for work authorization by filing Form I-765, Application for Employment Authorization.[42] Access to Asylum Division data through RAPS or PCQS may be granted to other offices within USCIS for the purpose of adjudicating the I-765. USCIS uses CLAIMS 3 to process applications for employment authorization.[43]

Fraud Detection

Information may also be referred to the FDNS Directorate, through manual or automated referral processes for screening and for investigation of fraud, public safety, or national security concerns. The DHS/USCIS/PIA-013-01 FDNS and DHS/USCIS/PIA-013 FDNS-DS PIAs provide an in-depth discussion of the FDNS Directorate and automated screening evaluating the privacy risks and mitigation strategies built into each process.[44]

Information Sharing

DHS created the DHS Data Framework, which is a scalable information technology program with built-in capabilities to support advanced data architecture and governance processes. This program will alleviate limitations associated with IT systems that are currently deployed

[40] See DHS/USCIS/PIA-016(a) CLAIMS 3 and Associated Systems, available at www.dhs.gov/privacy.
[41] See DHS/USCIS/PIA-063 Benefit Decision and Output Processes, available at www.dhs.gov/privacy.
[42] 8 C.F.R. §§ 274a.12(c)(8), 208.7.
[43] See DHS/USCIS/PIA-016(a) CLAIMS 3 and Associated Systems, available at www.dhs.gov/privacy.
[44] See DHS/USCIS/PIA-013-01 Fraud Detection and National Security Directorate (FDNS) and DHS/USCIS/PIA-013 Fraud Detection and National Security Data System (FDNS-DS), available at www.dhs.gov/privacy.

across multiple operational components in DHS. It will also enable more effective use and sharing of available homeland security-related information across the DHS enterprise and, as appropriate, the U.S. Government, while protecting privacy.[45] RAPS data is refreshed on a daily basis with the DHS Data Framework. As noted in the Data Framework PIA, to help mitigate the risk due to periodic refreshes, DHS requires users of the Framework to go back to the original DHS IT system and verify that an individual's information has not been updated pursuant to redress or correction before issuing any raw intelligence (e.g., intelligence information report), final analysis, or using the information operationally. Requiring users to verify information in the original DHS IT system will ensure that updates pursuant to redress or correction will be incorporated into any product, or before the information is used operationally.[46]

Asylum Pre-Screening System (APSS)

APSS is designed to serve as the primary system to manage, control, and track credible fear and reasonable fear screening cases for USCIS. Much like RAPS, APSS is used by officers to check the status of individual cases and by program managers to monitor the asylum pre-screening process as a whole. Each Asylum Officer or other designated asylum office representative is responsible for entering his or her cases into APSS as the case progresses. APSS is designed to provide the user with several different data entry screens that correspond to particular stages in the pre-screening process.

Referral

CBP or ICE refers individuals to a USCIS Asylum Office for a credible fear screening interview when such individuals are placed in expedited removal and express a fear of persecution or torture, an intention to apply for asylum, or a fear of return.[47] The Asylum Office enters information regarding the individual, the claim, and the determination into APSS. Individuals found to have a credible fear of persecution or torture are placed in INA § 240 removal proceedings before an Immigration Judge, where they may apply for asylum or other relief or protection from removal.[48] Individuals found not to have a credible fear of persecution or torture may request review of the negative determination by an Immigration Judge. If the individual does not request

[45] See DHS/ALL/PIA-046 DHS Data Framework, available at www.dhs.gov/privacy.
[46] See DHS/ALL/PIA-046(b) DHS Data Framework Appendix A – Approved Data Sets, available at www.dhs.gov/privacy.
[47] Certain aliens who are seeking admission and who are found inadmissible for engaging in fraud or willful misrepresentation, for making a false claim to U.S. citizenship, or for lacking valid documentation may be placed in expedited removal. See INA § 235 (b)(1); and 8 CFR §§ 208.30, 235.3.
[48] An alien is found to have a credible fear of persecution if there is a significant possibility, taking into account the credibility of the statements made by the alien in support of his or her claim and such other facts as are known to the officer, that the alien could establish eligibility for asylum under section 208 or for withholding of removal under section 241(b)(3). INA § 235(b)(1)(B)(v); 8 C.F.R. § 208.30(e)(2). An alien is found to have a credible fear of torture if he or she shows that there is a significant possibility that he or she is eligible for withholding of removal or deferral of removal under the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment ("Convention Against Torture"). 8 C.F.R. § 208.30(e)(3).

Immigration Judge review, or the Immigration Judge concurs with the negative determination, the individual may be removed.

CBP or ICE refers individuals to a USCIS Asylum Office for a reasonable fear screening interview when their prior order of deportation, exclusion, or removal is reinstated under INA § 241(a)(5) or they are subject to a final administrative removal order under INA § 238(b) and they express a fear of return to the country of removal or request withholding of removal.[49] The Asylum Office enters information regarding the individual, the claim, and the determination into APSS. Individuals found to have a reasonable fear of persecution or torture are placed in withholding-only proceedings before an Immigration Judge in which they may apply for withholding of removal under 241(b)(3) or withholding or deferral under the Convention Against Torture. Individuals found not to have a reasonable fear of persecution or torture may request review of the negative determination by an Immigration Judge. If the individual does not request Immigration Judge review, or the Immigration Judge concurs with the negative determination, the individual may be removed.

The Asylum Division receives information about individuals in the credible fear and reasonable fear processes through referral documentation provided by ICE or CBP, detailed on pages 3-4 above. In addition to the referral documentation, ICE or CBP may provide Form I-213, Record of Deportable/Inadmissible Alien, which contains personal information about the applicant, including information about the individual's entry into the United States and apprehension by DHS, as well as biographic and biometric information, including the applicant's name, address, date of birth, height, weight, sex, hair and eye color, occupation, photograph, and fingerprint. Form I-213 may also contain information about the individual's place of birth, nationality, and family members or associates.

Background, Identity, and Security Checks

In both the credible fear 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, identity, and security checks are automatically initiated for the applicant. APSS has automated background check capability for FBI name check and CBP TECS.

Pre-Screening Interview

Asylum Officers interview individuals during the reasonable fear and credible fear screening processes. Asylum pre-screening interviews may occur in person or remotely by telephone. Asylum Officers advise individuals in the credible fear and reasonable fear processes

[49] An alien is found to have a reasonable fear of persecution or torture if he or she establishes a reasonable possibility that he or she would be persecuted on account of his or her race, religion, nationality, membership in a particular social group or political opinion, or a reasonable possibility that he or she would be tortured in the country of removal. 8 C.F.R. § 208.31(c).

of their legal and procedural protections and receive specialized training on eliciting testimony through non-adversarial interviews. The individual's attorney or consultant[50] may be present at the interview, along with a government-contracted interpreter. At times, other Asylum Office staff may be present for performance review or training purposes. Asylum Officers take notes during the interview that are included in the applicant's A-File and serve as a reference for drafting the Asylum Officer's determination. The Asylum Officer may also elicit information about the applicant's attorney or consultant during the interview, which is recorded in APSS.

Determination

Credible fear and reasonable fear determinations are recorded using APSS following the pre-screening interview. Individuals in both processes are generally detained by ICE in detention facilities; however, some are not detained and their addresses are recorded in APSS. APSS also facilitates the printing of determination documents. Documentation of the final determination is placed in the A-File.

Additionally, Asylum Offices create and store 'working files' for credible and reasonable fear cases, which contain copies of referral documents and all documentation generated by the asylum office. The Asylum Division requires that Asylum Offices keep records of completed credible fear and reasonable fear cases. Credible Fear and Reasonable Fear working files may be disposed of by shredding if the Asylum Office Director concludes that the office lacks space to continue storing credible fear files; more than two months have passed since the credible fear determination was served or the case was closed; or six months have passed since the reasonable fear determination was served or the case was closed, the case has not been subjected to an unusual amount of scrutiny, and all necessary APSS updates to complete the case have been performed.

Statistical Reporting

All information maintained by RAPS and APSS is also replicated in the Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR).[51] Using a data repository such as eCISCOR allows RAPS and APSS data to be accessed in a read-only manner by other USCIS systems, accessible only to authorized users, for reporting, statistical analysis, and document production. eCISCOR transfers data from nearly all USCIS live transactional systems. Due to the age of many legacy USCIS live transactional systems and the high volume of cases they process, USCIS requires eCISCOR (and other backend storage systems)

[50] In the credible fear process, the individual may consult with any person of his or her choosing prior to the interview, and this have a consultant may be present during the interview. 8 C.F.R. § 208.30(d)(4). In the reasonable fear process, the individual may be represented by an attorney or accredited representative at the interview. 8 C.F.R. § 308.31(c).

[51] See DHS/USCIS/PIA-023(a) Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR), available at www.dhs.gov/privacy.

to reduce the labor and system strain involved in accessing, reporting, and sharing information between USCIS systems.

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?

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 title 8 of the Code of Federal Regulations (CFR).

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 – 240.70, 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.

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 information by the Asylum Division:

- The Alien File, Index, and National File Tracking System SORN covers the information maintained in the A-File, including hardcopy records of asylum applications, NACARA § 203 applications, credible fear screenings, reasonable fear screenings, and supporting documentation. USCIS creates an A-File for each indvidual.[52]
- Background Check Service[53] covers background checks and their results; and

[52] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System, 78 FR 69864 (November 21, 2013).
[53] DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007).

- The Asylum Information and Pre-Screening SORN covers the collection, use, and maintenance of asylum applications, NACARA § 203 applications, credible fear screenings, and reasonable fear screenings.[54]

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

RAPS and APSS are minor applications under the USCIS Mainframe Applications accreditation boundary. USCIS completed the security assessment and authorization documentation for the USCIS Mainframe Applications in October 2015, and was issued an authority to operate until September 2017. The USCIS Mainframe Applications are planned to enter the Ongoing Authorization program during the recertification process.

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

USCIS stores the physical documents (i.e., applications and referral documents) and supplemental documentation in the Alien File and processes benefit requests in the respective case management systems. The A-File [N1-566-08-11] records are permanent whether hard copy or electronic. USCIS transfers the A-Files to the custody of NARA 100 years after the individual's date of birth.

NARA approved the RAPS [N1-563-04-06] and APSS [N1-563-04-07] Retention Schedule. Master File automated records are maintained for 25 years after the case is closed, then archived for 75 years, and then destroyed. Reports used to facilitate case processing that contain personally identifiable information will be maintained at Headquarters and Asylum Field Offices and destroyed when no longer needed.

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.

Forms associated with affirmative asylum and NACARA § 203 are subject to the Paperwork Reduction Act. These forms include:

- Form I-589, Application for Asylum and Withholding of Removal (OMB No. 1615-0076);
- Form I-870, Record of Determination/Credible Fear Worksheet (pending OMB approval);

[54] DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (Nov. 30, 2015).

- 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
- Form I-899, Record of Determination/Reasonable Fear Worksheet (pending OMB approval).

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested or collected, as well as reasons for its collection.

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

Information about asylum applicants, NACARA § 203 applicants, credible and reasonable fear screening interviewees, beneficiaries, and family members includes:

- Name;
- Alias(es);
- Birth Date(s);
- A-Number;
- Receipt Number;
- SSN (if available);
- Address/residence in the United States;
- Foreign residence history;
- Detention location (if detained by ICE);
- Phone Number;
- Gender;
- Marital Status;
- Place of Marriage;
- Date of Birth;
- Country of Birth;
- Country of Nationality (or nationalities);
- Ethnic Origin;

- Religion;
- Port(s), date(s) of entry, and status at entry(ies);
- Filing date of asylum, NACARA § 203, or follow-to-join application;
- Education history;
- Work history;
- Results of security checks;
- Language(s) spoken;
- Claimed basis of eligibility for benefit(s) sought;
- Case status;
- Case history;
- Employment authorization eligibility and application history;
- Government-issued identification (e.g., passport):
  - Document type;
  - Issuing organization;
  - Document number;
  - Expiration date; or
  - Benefit requested.
- Notices and communications, including:
  - Appointment notice(s);
  - Receipt notice(s);
  - Requests for evidence;
  - Notices of Intent to Deny (NOID);
  - Decision notices and assessments; or
  - Proofs of benefit.
- Records regarding military service, organization membership, or affiliation;
- Criminal history or involvement in criminal activites (e.g., arrests/detentions, involvement with national security threats, criminal offenses, persecution, torture, genocide, killing, injuring, forced sexual contact, limiting or denying others religious

beliefs, service in military or other armed groups, work in penal or detention systems, weapons distribution, combat training);

- Education and employment history;
- Tax records;
- Explanation/description of foreign travel;
- Signature;
- Supporting documentation as necessary (e.g., birth, marriage, or divorce certificates, licenses, explanatory statements, and unsolicited information submitted voluntarily by the applicant or family members in support of a benefit request);
- Photographs and other biometrics (e.g., fingerprints);
- Results from criminal and national security background check information (CBP TECS Check, EARM Check, FBI Fingerprint/Name Check, OBIM/IDENT Check, DoD ABIS Check, NCTC Check); and
- Final Decision.

Information about Attorneys, Accredited Representatives, and Form Prepares includes:

- Name;
- Law firm/recognized organization;
- Physical and mailing address(es);
- Phone and fax number(s);
- Email address;
- Attorney bar card number or equivalent;
- Bar membership;
- Accreditation date;
- Board of Immigration Appeals (BIA) representative accreditation;
- Expiration date;
- Law practice restriction explanation; and
- Signature.

Information about Preparers and Interpreters may include:

- Name;
- Organization;
- Business state ID number;
- Physical and mailing address(es);
- Email address;
- Phone and fax number(s);
- Relationship to benefit requestor; and
- Signature.

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

A majority of data maintained by the Asylum Division is obtained directly from the individual applicant in the application or during the interview. Information regarding an asylum applicant's dependent spouse and children included in the application will be housed in RAPS, and for individuals in the credible fear process, information about their spouse and children may be housed in APSS. Applicant's dependent spouse and children have a right to an individual determination, but if the applicant has a positive determination, the applicant's dependent spouse and children may be included on the positive determination without resolving their individual claim. RAPS and APSS receive background check information from systems described under "Background, Identity, and Security Checks" above.

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

During the course of any adjudication, Asylum Office staff may use commercial record systems (i.e., LexisNexis Law Enforcement Systems, Accurint, and ChoicePoint's AutotrackXP) to investigate the veracity of a benefit application. Asylum Office staff may also use publicly available systems such as online search engines, news media, or social media to assist with the adjudication of a claim. Commercial sources and publicly available data is compared with applicant-reported information regarding when the applicant entered the country, how long the applicant has been in the United States, and when the applicant encountered harm outside the United States. If the Asylum Division has information from a commercial data provider that is inconsistent with relevant information provided by the applicant, the Asylum Officer must

confront the applicant with that information and provide him or her with the opportunity to explain the inconsitency. No commercial or publicly available information is transmitted to or stored in RAPS or APSS. In accordance with Asylum Division policy, for any case in which provided commercial data is used in an adjudication and in any way impacts the decision, the record must be printed and placed in the A-File.

2.4 Discuss how accuracy of the data is ensured.

The USCIS Service Centers follow standard operating procedures (SOP) in order to enter asylum and NACARA applications into RAPS. All applicants within the jurisdiction of an Asylum Office receive a personal interview prior to the full adjudication of their benefit applications. 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 supervisory review or quality assurance review prior to a final determination. 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 or corrected information.

RAPS and APSS are designed to require specific entries in the sequence outlined by the operating procedures to prevent inconsistencies in applicant data and decision processing entries. RAPS and APSS accomplish this quality control through program coding that allows or prevents record updates based on defined parameters. For example, if a security check 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 program coding exists for case closures, case transfers, file maintenance, and many other case processing tasks. Furthermore, standard recurring 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.

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 throughout the adjudication process.

Mitigation: USCIS partially mitigates this risk through training, supervisory reviews, and ongoing quality assurance reviews. The USCIS Affirmative Asylum Procedures Manual[55] 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 DHS mainframe

[55] https://www.uscis.gov/sites/default/files/USCIS/Humanitarian/Refugees%20%26%20Asylum/Asylum/AAPM-2016.pdf.

tables verify that the appropriate state or code has been selected). Authorized USCIS Asylum Division personnel have the ability to correct inaccuracies in RAPS and APSS. To maintain quality and consistency in processing benefit request forms, Asylum Division employees receive training on these procedures.

Privacy Risk: There is a risk of over collection of information during the course of the application and interview processes.

Mitigation: The USCIS Office of Privacy reviews each immigration form during the form development or promulgation 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.

The information collected from the Form I-589 and Form I-881 applications is required to adjudicate the asylum and NACARA § 203 benefits. Asylum Officers are trained to elicit testimony during asylum and protection screening interviews using lines of questioning relevant to adjudicating the benefit or conducting the protection screening. RAPS and APSS allow the entry of only the minimum data required to track the processing of 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 Form I-589, Application for Asylum and for Withholding for Removal. All information requested in the applications and testimony elicited during interviews is relevant to ensure that bona fide applicants are identified, to prevent benefit fraud, and to enable offices to adjudicate and serve decisions at the individual's appropriate address.

Privacy Risk: There is a risk that information in RAPS and APSS that is replicated and shared via eCISCOR is not updated in real time, and therefore may be inaccurate.

Mitigation: This risk cannot be mitigated. USCIS uses eCISCOR to share RAPS and APSS information more efficiently with other USCIS systems for interoperability purposes. If constant queries were performed against RAPS and APSS, which are live transaction systems designed to perform real-time daily tasks for USCIS customers, the primary source system functionality would significantly decrease. The RAPS and APSS systems lag would cause considerable mission disruption. Therefore, USCIS relies on eCISCOR to perform queries. To mitigate the risk of inaccurate data within eCISCOR, eCISCOR refreshes from RAPS, APSS, and other source systems on a daily basis (generally overnight).

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

Specific uses of RAPS and APSS data include:

- Correctly recording and identifying the applicant and to verify the accuracy of information provided in an application (including the information on derivative spouses and children);
- Generating and sending correspondence (e.g., interview notice, denial, grant, or requests for additional information) to the applicant, derivatives, and legal representative, if any;
- Facilitating and maintaining security screening check results to determine suitability for asylum benefits using criminal, immigration, or terrorism-related history;
- Managing adjudicative workflow; and
- Generating 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?

USCIS provides the following non-USCIS DHS components read-only access to Asylum Division information and records: (1) CBP, for border and inspection processing (to confirm immigration status); (2) ICE, for investigatory, removal, and immigration court functions; and (3) the Office of the Citizenship and Immigration Services Ombudsman, for providing individual case assistance to the public. Asylum Division information is also used to respond to queries from DHS law enforcement intelligence analysts upon request.

Other DHS agencies that may receive Asylum Division information and records include the following components:

- The Office of Inspector General (OIG) may be given Asylum Division information and records during the course of an audit, investigation, or inspection.
- The Office of Legislative Affairs (OLA) may be given information in the course of in inquiry.
- The Office of Citizen and Citizenship and Immigration Services Ombudsman may be given information in the course of an inquiry lodged by an applicant.
- The Office of the General Counsel (OGC) may be given information in the course of an investigation, during litigation, or for an assessment of a legal issue.
- The 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, as well as audits and inquiries by the DHS Secretary may require the release of Asylum Division information and records to other DHS components on an ad hoc basis.
- The Office of Immigration Statistics (OIS) may receive Asylum Division data in the course of developing, analyzing, and disseminating statistical information needed to inform immigration policy.

Biographic information available in Asylum Division data and statistical reports may be shared with the above-listed DHS components for the purposes of evaluating eligibility for a benefit, litigation, and policymaking.

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: To ensure the information is used consistently with the purposes of the original collection, only personnel with the proper security clearance and a need for the information are granted access to RAPS, APSS, and PCQS. The system administrator is responsible for granting the appropriate level of access. All users will be properly trained on the use and release of information in accordance with agency policies, procedures, regulations, and guidance. In addition, DHS personnel are required to take annual computer security and privacy awareness training. All authorized users access RAPS and APSS with unique log-on credentials so that changes to information in the system can be tracked using the user ID.

Privacy Risk: There is a risk that unauthorized users may gain access to information in RAPS, APSS, and PCQS.

Mitigation: Records are protected by administrative, physical, and technical safeguards. Access to data is granted to only a limited number of users for mission-related purposes. USCIS grants access based on the user's job function and duty station. The user interfaces for RAPS, APSS, and PCQS are available only via specific government-furnished equipment or workplace as a service (WPaaS) accessed using the employee's Personal Identity Verification (PIV) card. USCIS offices where this equipment is available are located in buildings staffed with 24-hour security service and other security mechanisms. USCIS restricts access to the premises to those provided with 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.

Employees with an active, approved telework agreement may work remotely using government-furnished equipment or WPaaS technology accessed using the employee's PIV card. Teleworking employees must complete telework training and are responsible for ensuring that records subject to the Privacy Act and other sensitive or classified data are not disclosed to anyone except those who are authorized to access such information in order to perform their duties. All teleworking employees complete an attestation that they will apply approved safeguards to protect government records from unauthorized disclosure or damage and will comply with the Privacy Act requirements set forth in the Privacy Act of 1974, codified in 5 U.S.C. 552a, and other similar security and privacy requirements.

Employees are to report all PII security violations to their supervisor immediately upon discovery of the incident. No classified documents (hardcopy or electronic) may be taken to an employee's alternative worksite and electronic Sensitive But Unclassified (SBU) information, including PII and For Official Use Only (FOUO) data, may only be accessed with government-furnished equipment or through workplace as a service (WPaaS) technology. When not in use, electronic and hardcopy SBU and sensitive personal property must be kept in a locked container, drawer, or file cabinet accessible only by individuals determined to have a need-to-know in accordance with the applicable management directives.

The specific user must have been provided the proper secondary access user roles, as described in Section 8.0 Auditing and Accountability, to view RAPS or APSS before the systems are visible through the user interface.

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.

The instruction associated with affirmative asylum and NACARA § 203 forms contains a Privacy Notice. Each Privacy Notice provides notice to individuals about the Agency's authority to collect information, the purposes of data collection, how USCIS will share information outside of the Department, and the consequences of declining to provide the requested information to USCIS. The forms also contain a provision by which an applicant authorizes USCIS to release any information received from the benefit requestor or beneficiary as needed to determine eligibility for benefits.

Individuals referred for credible fear and reasonable fear screenings do not provide documents or file an application with USCIS. ICE and CBP refer these individuals to USCIS for screening via documents that are a part of the removal process, as described in the Overview to this PIA. Individuals in the credible fear and reasonable fear processes receive an orientation explaining the process, which is documented on the M-444 (credible fear) and M-488 (reasonable fear). As these individuals are already subject to an order of removal (expedited removal for credible fear, reinstatement of a prior order or a final administrative removal order for reasonable fear), the individuals do not complete a benefit application with USCIS.

Individuals receive general notice through this PIA, DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking SORN, and DHS/USCIS-010 Asylum Information and Pre-Screening SORN.

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

Through the application process, individuals have consented to the use of the information submitted for adjudication purposes. Applicants who apply for affirmative asylum and NACARA § 203 have an opportunity and right to decline to provide information. USCIS benefit applications require the applicant to provide biographic or biometric information. This information is critical in making an informed adjudication decision to grant or deny an immigration benefit. Failure to submit such information prohibits USCIS or EOIR from processing and properly adjudicating the application and thus precludes the applicant from receiving the requested benefit.

Applicants in the credible fear or reasonable fear process may dissolve or withdraw their claim and accept removal. Applicants may also refuse to provide information, which may lead to a negative determination if such information is material to the adjudication.

4.3 Privacy Impact Analysis: Related to Notice

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 application for benefits. USCIS provides notice to individuals through a Privacy Notice, this PIA, and the associated SORN.

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.

USCIS stores the physical documents and supplemental documentation in the A-File and processes asylum requests in the respective case management system. The A-File [N1-566-08-11] records are permanent whether hard copy or electronic, until destroyed. USCIS transfers the A-Files to the custody of NARA 100 years after the individual's date of birth.

NARA approved the RAPS [N1-563-04-06] and APSS [N1-563-04-07] Retention Schedule. Master File automated records are maintained for 25 years after the case is closed, then archived for 75 years, and then destroyed. USCIS is proposing to update the RAPS and APSS Retention Schedule to maintain data for 100 years and then destroy the information to align with the approved A-File schedule. This retention schedule allows the individual to adjust status and naturalize. It also allows USCIS to timely address any follow-up inquiries (e.g., requests related to security inquiries and Freedom of Information Act/Privacy Act matters).

5.2 Privacy Impact Analysis: Related to Retention

There is no risk associated with retention in relation to Asylum Division data. USCIS is adhering to the NARA-approved RAPS and APSS Retention Schedule. Although there is always an inherent risk in retaining information for any length of time, the RAPS and APSS information retention periods are consistent with the concept of retaining information only for as long as necessary to support the agency's mission. USCIS has designated asylum data as a permanent status since the benefit is subject to termination in the future and individuals can apply to adjust status at any time.

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.

Asylum Division information and records may be shared with outside entities, either pursuant to regulation or through specific agreements.

Department of Justice (DOJ) – Executive Office for Immigration Review

The Asylum Division inputs case information into the Department of Justice Executive Office of Immigration Review (EOIR) Case Access System for EOIR (CASE) when referring an applicant to immigration court for proceedings.[56] The Asylum Division may also share Asylum Division information and records, including individual or statistical data, with EOIR on a case-by-case, ad hoc basis for the purposes of evaluating eligibility for a benefit[57] or removability, evaluating procedures, litigation, and policymaking.[58]

Respondents in removal proceedings who file an I-589, Application for Asylum and for Withholding of Removal, are instructed to file the first three pages of the I-589 and a Form EOIR-28, Notice of Entry of Appearance as Attorney or Representative Before the Immigration Court, if applicable, with USCIS. USCIS inputs information from I-589 applications filed as a defense to removal into a separate section of RAPS, referred to as the "defensive" side of RAPS. RAPS initiates FBI name checks and FBI fingerprint checks for defensive filings, and receives IDENT results from OBIM. The results of these security checks may be shared with DOJ EOIR.

Department of Justice – Other Components

Records may be shared with the FBI and any other U.S. Government official or contractor having a need to examine information in connection with any U.S. Government investigation concerning any criminal or civil matter (e.g., fingerprint and name checks). Records may also be shared for litigation purposes with the DOJ Office of Immigration Litigation (OIL).

[56] See Privacy Impact Assessment for Case Access System for EOIR (CASE), available at https://www.justice.gov/sites/default/files/opcl/docs/eoir_pia.pdf.
[57] This includes, but is not limited to, tracking days accrued and stoppages of the 180-day Asylum Employment Authorization Document (EAD) Clock.
[58] See Memorandum of Agreement Between the Department of Homeland Security and The Department of Justice Executive Office for Immigration Review Regarding the Sharing of Information on Immigration Cases, October 22, 2012, available at: https://www.justice.gov/sites/default/files/eoir/legacy/2014/11/20/DHS-MOA-Data-Agreement.pdf.

National Counter Terrorism Center (NCTC)[59]

DHS has entered into an updated Memorandum of Agreement (MOA)[60] with NCTC in order to facilitate NCTC's counterterrorism efforts and to identify terrorism information within RAPS.[61] Pursuant to 8 CFR § 208.6(a), the Secretary has authorized regular sharing of asylum-related information for this purpose. This information sharing also aligns with DHS's mission to prevent and deter terrorist attacks and helps to ensure that immigration benefits are not granted to individuals who pose a threat to national security.

NCTC replicates RAPS information into its Counterterrorism Data Layer (CTDL) to support its counterterrorism efforts. The CTDL provides NCTC analysts with "the ability to search, exploit, and correlate terrorism information in a single environment." For example, NCTC analysts may run queries against RAPS information in the CTDL to identify terrorism information within RAPS. When RAPS information is determined to constitute terrorism information, NCTC will provide feedback to DHS, which DHS may use to support its mission to prevent and deter terrorist attacks. Additionally, when NCTC replicates RAPS information, the records will be marked with a "time-to live" date, which will specify when the RAPS information will be deleted if it is not identified as terrorism information.

Additionally, NCTC conducts automated screening of all RAPS information to generate potential leads that may constitute terrorism information. NCTC analysts review all of the potential leads to determine whether the RAPS information constitutes terrorism information. NCTC processes all RAPS records through this screening support process within the "temporary retention" period of three years to determine whether RAPS records constitute terrorism information. This screening activity supports DHS's mission to prevent and deter terrorist attacks and assists DHS in its assessment of the national security risk that may be posed by granting asylum status to applicants. Because this screening support assists DHS, the MOA includes provisions to allow DHS, in coordination with NCTC, to perform the review of the automated matches if NCTC resources or workload prioritization preclude NCTC from providing this review.

---

[59] See DHS/USCIS/PIA-027(b) Refugees, Asylum, and Parole System and the Asylum Pre-Screening System, available at www.dhs.gov/privacy.

[60] The MOA does not include the APSS database.

[61] DHS Delegation Number 08505, Delegation of Authority to Disclose Asylum and Refugee Information, vests the authority to disclose Asylum and Refugee Information to the Under Secretary for Intelligence and Analysis, the Assistant Secretary of United States Citizenship and Immigration Services, the Commissioner of U.S. Customs and Border Protection, the Director of United States Immigration and Customs Enforcement, and the Director of Operations Coordination for counterterrorism and intelligence purposes. This delegation does not affect the disclosure of Asylum and Refugee Information in accordance with the provisions of Title 8, Code of Federal Regulations (C.F.R.), Section 208.6(c). Section 208.6, "Disclosure to third parties," provides that such authority will be exercised only for authorized intelligence or counterterrorism functions and in accordance with policies and procedures established by the Under Secretary for Intelligence and Analysis in consultation with the other officials named in the delegation.

NCTC reviews, retains, and disseminates RAPS records it has determined to constitute terrorism information in accordance with procedures approved for NCTC by the Attorney General in accordance with Section 2.3 of Executive Order 12333, and additional terms specified in the MOA.

Department of Defense (DoD)

Pursuant to a Memorandum of Agreement between the Department of Defense (DoD) and the Department of Homeland Security (DHS), biometrics information is shared between USCIS and DoD in order to support the missions of both agencies. All affirmative asylum applicants appear at an Application Support Center (ASC) for biometrics collection and those biometrics are transmitted to DoD Automated Biometric Identification System (ABIS).[62] DoD/ABIS then conducts a search of all ABIS record categories on the received biometrics. DoD/ABIS will record the RAPS data, and a listed source of "DHS record" in ABIS indicating that the check took place. To preserve the confidentiality of the asylum application, no indication is made of the asylum application or asylum program office. The results of the check are returned, indicating whether the check resulted in a fingerprint match, no matching record, an error report, or a duplicate check. All results will include the information submitted by USCIS, the results of the check, all ABIS matching records, and the date of the ABIS check. The check requests will be returned to USCIS systems. Whether the DoD/ABIS check resulted in a match is displayed in RAPS. Asylum Officers review the ABIS results in CPMS prior to interview and consider the information in performing the benefit adjudication.

Five Country Conference (FCC)

The DHS Secretary authorized the Asylum Division to permit regular sharing of asylum-related information with the Five Country Conference (FCC), a forum for cooperation on migration and border security between the countries of Australia, Canada, New Zealand, the United Kingdom, and the United States. Under the auspices of the FCC, IDENT, via the Office of Biometrics Management (OBIM), supports the exchange of biometric information in specific immigration cases. The biometrics exchanges are searched against the holdings of each FCC partner to determine the existence of information that may be pertinent to asylum adjudication officers and their supervisors. Such information may include previous or current immigration status, asylum application materials, and responses to additional inquiries from FCC partners. The Secretary has authorized disclosure of asylum-related information with the FCC partner countries.

Government of Canada

The United States and the Government of Canada also share asylum-related information bilaterally through an arrangement formalized in a Statement of Mutual Understanding on

[62] Department of Defense Detainee Biometric Information System, 72 FR 14534 (Mar. 28, 2007). Also Defense Biometric Services, 74 FR 48237 (Sept. 22, 2009).

Information Sharing (SMU) and an asylum-specific Annex to the SMU, which together permit Canada's Department of Citizenship and Immigration Canada (CIC)[63] and USCIS to exchange asylum-related biographic and biometric records on both a case-by-case and systematic basis.

Asylum Division information and records 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. As noted above, the DHS Secretary has authorized similar disclosure under agreements with the United Kingdom and Australia for specific projects.

Department of Health and Human Services (HHS)

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 consists of the name, date of birth, A-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 zipcode, 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.

Department of State (DOS)

The U.S. Department of State has access to review limited RAPS records through USCIS's PCQS. PCQS allows DOS users to search for applicant records in RAPS as well as other USCIS systems of records. The access is provided as an addendum to pre-existing Memorandum of Understanding (MOU) between the Department of State Bureau of Consular Affairs and DHS USCIS, for the exchange of visa and immigration data.

Other Disclosure to U.S. Government Offices and Foreign Governments

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,

[63] CIC has since been renamed Immigration, Refugees, and Citizenship Canada (IRCC).

then the requested information is generally provided without regard to the regulation at 8 C.F.R. § 208.6. Written requests for asylum-related information by individual members of Congress or their respective staff members are considered on a case-by-case basis. Requests made by any foreign government are handled in accordance with 8 C.F.R. § 208.6 and appropriate delegations of the Secretary's waiver authority.

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

DOS

Sharing USCIS data with DOS is compatible with the purpose of the system because the DOS mission, like USCIS, includes ensuring lawful visits and immigration to the United States as dictated by the INA. Routine Use K of the Asylum Information and Pre-Screening SORN and Routine Use O of the A-File SORN permit USCIS to share information with the DOS for the purpose of assisting in the processing of benefit requests under the INA, and all other immigration and nationality laws including treaties and reciprocal agreements.

HHS

Sharing USCIS data with HHS is compatible with the purpose of the system because Sections 400.203(b) and 400.211 of 45 Code of Federal Regulations provide access to medical benefits for individuals granted asylum. All asylees are eligible to apply for ORR assistance and services under the policy. Routine Use L of the Asylum Information and Pre-Screening SORN and Routine Use BB of the A-File SORN permit USCIS to share information with the HHS to provide emergency relief to qualified asylees, meet congressional reporting requirements, provide post-decisions services, and generate statistical reports for allocating funding for asylee social benefits.

NCTC

Sharing USCIS data with NCTC is compatible with the purpose of the system because USCIS is required to conduct background and security checks to identify threats to national security and public safety posed by those seeking immigration benefits. Routine Use H and I of the Asylum Information and Pre-Screening SORN and EE of the A-File SORN permit USCIS to share information with NCTC or to any element of the U.S. Intelligence Community, or any other federal or state agency having a counterterrorism function, provided that the need to examine the information, or the request is made in connection with its authorized intelligence or counterterrorism functions and the information received will be used for the authorized purpose for which it is requested.

Government of Canada

Sharing USCIS data with Canada is compatible with the purpose of the system because this information sharing intiative is intended to enhance the cooperation between the United States and Canada to prevent terrorism, including terrorist travel, serious crime and other threats to national security, and to assist in the administration and enforcement of immigration laws. Routine Use J of the Asylum Information and Pre-Screening SORN and Routine Use CC of the A-File SORN permits USCIS to share information with the Government of Canada for the purpose of verifying or ascertaining the citizenship or immigration status of any individual within the jurisdiction of the agency, for any purpose authorized by law as limited by the terms and conditions of 8 CFR § 208.6 and any waivers issued by the Secretary pursuant to 8 CFR § 208.6.

DOJ

Sharing USCIS data with DOJ is compatible with the purpose of the system because DOJ administers the nation's immigration court system. Routine Use A of both the Asylum Information and Pre-Screening and A-File SORNs permit USCIS to share information with the Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and when DHS, DOJ, or any current or former employee of DHS or DOJ are a party to the litigation or has an interest in such litigation.

FCC

Sharing USCIS data with FCC is compatible with the purpose of the system because these information sharing initiatives are to enhance the cooperation between the United States and its foreign partners to prevent terrorism, including terrorist travel, serious crime and other threats to national security, and to assist in the administration and enforcement of immigration laws. Routine Use J of the Asylum Information and Pre-Screening SORN and Routine Use CC of the A-File SORN permit USCIS to share information with the FCC for the purpose of verifying or ascertaining the citizenship or immigration status of any individual within the jurisdiction of the agency for any purpose authorized by law as limited by the terms and conditions of 8 CFR § 208.6 and any waivers issued by the Secretary pursuant to 8 CFR § 208.6.

DoD

Sharing USCIS data with DoD is compatible with the purpose of the system because USCIS is required to conduct background and security checks to identify threats to national security and public safety posed by those seeking immigration benefits. Pursuant to Routine Use G of Biometric Storage System of Records Notice, all or a portion of the records or information contained in USCIS's biometrics storage system may be disclosed outside DHS as a routine use to federal and foreign government intelligence or counterterrorism agencies when DHS reasonably believes there to be a threat or potential threat to national or international security for which the

information may be useful in countering the threat or potential threat, when DHS reasonably believes such use is to assist in anti-terrorism efforts, and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

USCIS may also share information with federal, state, local, and foreign government agencies and authorized organizations in accordance with approved routine uses, as described in the associated published system of records notices.

6.3 Does the project place limitations on re-dissemination?

Yes. 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., DOJ, DoD, DOS, FCC, Canada) 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 require the receiving entity to 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 DHS's permission, as applicable.

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

USCIS keeps an electronic record in system audit logs, emails, and A-File records of all RAPS and APSS records sent to non-DHS partners.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk of unauthorized access to RAPS or APSS.

Mitigation: To ensure the information is used consistently with the purposes of the original collection, Asylum Division personnel strictly control the process of data sharing. All prospective users must be authorized to gain access to information contained within RAPS, APSS, or PCQS. All users 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. U.S. Government employees must undergo annual security and privacy awareness training.

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 the Asylum Information and Pre-Screening SORN. USCIS documents these safeguards in MOU/MOA with the external partners. 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 with an external agency.

Privacy Risk: There is a risk that USCIS may disclose protected information inconsistent with the confidentiality requirements of 8 CFR § 208.6.

Mitigation: DHS employees are aware of the importance of safeguarding information protected by 8 CFR § 208.6. All employees with access to protected asylum information in RAPS, APSS, or PCQS must read and sign an acknowledgement of confidentiality obligations concerning asylum-related information. The confidentiality obligations acknowledgment form contains the text of 8 CFR § 208.6 and a detailed explanation of the confidentiality obligations. Employees must agree to comply with these obligations before receiving access to asylum information in RAPS, APSS, or PCQS. This mitigates the risk by ensuring that all employees are familiar with the confidentiality obligations under 8 CFR § 208.6 and agree to abide by them.

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, or filing complaints.

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

Any individual, regardless of citizenship status, may gain access to his or her USCIS records by filing a Freedom of Information Act (FOIA) request. U.S. Citizens and Lawful Permanent Residents may also file a Privacy Act request to access their information. If an individual would like to file a FOIA or 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, however, be exempt from disclosure under the Privacy Act or FOIA applicable exemptions. Requests for access to asylum, NACARA § 203, reasonable fear,

and credible fear records will be reviewed on a case-by-case basis. 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 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. Persons not covered by the Privacy Act are not able to amend their records through FOIA. Should a non-U.S. person find inaccurate information in his or her record received through FOIA, he or she may visit a local USCIS Field Office to identify and amend inaccurate records with evidence.

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 this PIA, Privacy Notice, and through the USCIS website. Specifically, the SORNs set forth in Section 1.2 provide individuals with guidance regarding the procedures for correcting information. The Privacy Notice including notice of an individual's right to correct information, are also contained on the instructions to immigration forms published by USCIS.

7.4 Privacy Impact Analysis: Related to Redress

There is no risk associated with redress in relation to RAPS and APSS. USCIS provides individuals with access to their records in RAPS and APSS when requested through a FOIA or Privacy Act request. The information requested may be exempt from disclosure under the Privacy Act because information contained within RAPS and APSS may contain law enforcement sensitive information, the release of which could compromise ongoing criminal investigations.

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?

USCIS Asylum Division ensures that practices stated in this PIA comply with internal USCIS policies, including the USCIS privacy policies, SOPs, orientation and training, rules of behavior, and auditing and accountability. RAPS and APSS include an audit trail capability to

monitor user activities and generate alerts for unauthorized access attempts. The general audit log and the security log allow the Global Administrator to select event type, such as access or logon, and the data displayed includes timestamp, name, Internet Protocol address, transaction, and site. The other log is the auto lock log and the display for it shows the employee's name, last login, auto lock date with time, reinstate date with time, username, and site. This auditing is a strong influence for users to use RAPS and APSS appropriately.

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 compliance with federal law and regulations, users have access to Asylum Division information and records 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. A user desiring access must complete a Form G-872A, Request for PICS Mainframe Applications, for access to RAPS or APSS. This application states the justification for the level of access being requested. The requestor's supervisor and the Password Issuance and Control System (PICS) officer review this request; if approved, the requestor's clearance level is independently confirmed and the user account established. Secondary access is then provided by the USCIS Asylum Division, or for Service Center or National Benefits Center personnel, by local administrators at those locations. Those local administrators determine the specific user roles based on the user's job duties and need-to-know. System Administrators and contracted developers may have access if they are cleared and have legitimate job functions. 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.

There are several Department and government-wide regulations and directives that provide

additional guidance. 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, APSS, or PCQS, except under certain limited circumstances. All users must sign a confidentiality acknowledgement in order to obtain any access to RAPS, APSS or PCQS.

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 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 Information Security Officer, Office of the Chief Counsel, and the respective program office.

Responsible Officials

Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Privacy Impact Assessment Update
for the

USCIS Asylum Division

DHS/USCIS/PIA-027(d)

September 27, 2018

Contact Point
Donald K. Hawkins
Privacy Officers
U.S. Citizenship and Immigration Services
(202) 272-8000

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Asylum Division of the U.S. Citizenship and Immigration Services (USCIS) adjudicates applications for asylum, benefits pursuant to Section 203 of the Nicaraguan Adjustment and Central American Relief Act (NACARA § 203), withholding of removal under the terms of a settlement agreement reached in a class action,[1] and screening determinations for safe third country, credible fear, and reasonable fear. The Asylum Division historically used the Refugees, Asylum, and Parole System (RAPS) and the Asylum Pre-Screening System (APSS) in support of its mission critical functions. Both systems were originally developed by the former Immigration and Naturalization Service (INS). The Asylum Division is seeking to retire APSS and RAPS and use Global, operating in a cloud-based environment, to serve as the primary IT case management system for the administration of affirmative asylum, NACARA § 203, withholding of removal under the terms of a settlement agreement reached in a class action, credible fear, and reasonable cases. USCIS is updating this Privacy Impact Assessment (PIA) because the Asylum Division uses the new cloud-based Global system and has migrated records, containing personally identifiable information (PII), from APSS and RAPS into Global in order to conduct its adjudications.

Overview

USCIS oversees lawful immigration to the United States. As set forth in Section 451(b) of the Homeland Security Act of 2002, Public Law 107-296, Congress charged USCIS with administering the asylum program. USCIS, through its Asylum Division, administers the affirmative asylum program to provide 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 Section 208 of the Immigration and Nationality Act (INA), 8 U.S.C. § 1158 and 8 CFR Part 208. The USCIS Asylum Division also adjudicates the benefit program established by the Nicaraguan Adjustment and Central American Relief Act (NACARA) § 203[2] and administers safe third country, credible fear, and reasonable fear screening processes.[3]

The Asylum Division supports the following four programs:

1. Asylum

Every year people come to the United States seeking protection because they have suffered persecution or fear that they will suffer persecution on account of race, religion, nationality, membership in a particular social group, or political opinion. The two ways to obtain asylum in

[1] American Baptist Churches v. Thornburgh, 760 F. Supp. 796 (N.D. Cal. 1991) (ABC Settlement).
[2] Pub. L. No. 105-100, 111 Stat. 2193 (1997), amended by Pub. L. No. 105-139, 111 Stat. 2644 (December 2, 1997).
[3] Section 203 of Pub. L. No. 105-100.

the United States are through the affirmative process before USCIS, and the defensive process before an immigration judge in the Executive Office for Immigration Review in the Department of Justice (EOIR). To obtain asylum, the individual must be physically present in the United States. Generally, an individual may apply for affirmative asylum status regardless of how he or she arrived in the United States or his or her current immigration status. An individual may include his or her spouse and/or unmarried children present in the United States as derivatives on his or her asylum application. A defensive application for asylum occurs when an individual requests asylum as a defense against removal from the United States. In defensive asylum cases, the individual is currently in removal proceedings in immigration court with EOIR.

USCIS is responsible for the administration and adjudication of the affirmative asylum process. Individuals granted asylum status possess this status indefinitely, may work in the United States, may request derivative status for immediate family members within two years of the grant of asylum status, and may apply for permanent residence after one year.

2. Nicaraguan Adjustment and Central American Relief Act (NACARA Section 203)

Section 203 of NACARA applies to certain individuals from Guatemala, El Salvador, and the former Soviet bloc countries (the Soviet Union or any republic of the former Soviet Union, such as Russia, Latvia, Lithuania, Estonia, Albania, Bulgaria, the former Czechoslovakia, the former East Germany, Hungary, Poland, Romania, or Yugoslavia or any state of the former Yugoslavia) who entered the United States and applied for asylum by specified dates or registered for benefits. Section 203 of NACARA allows qualified individuals to apply for suspension of deportation or for special rule cancellation of removal under the standards similar to those in effect before the Illegal Immigration Reform and Immigrant Responsibility Act of 1996. If granted, individuals receive lawful permanent resident status.

3. Credible Fear Screenings

Section 235 of Immigration and Nationality Act (INA), as amended, and its implementing regulations provide that certain categories of individuals are subject to expedited removal without a hearing before an immigration judge. These include: arriving stowaways; certain arriving aliens at ports of entry who are inadmissible under section 212(a)(6)(C) of the INA (because they have presented fraudulent documents or made a false claim to USCIS or other material misrepresentations to gain admission or other immigration benefits) or 212(a)(7) of the INA (because they lack proper documents to gain admission); and certain designated aliens who have not been admitted or paroled into the United States.

Individuals subject to expedited removal who indicate an intention to apply for asylum, express a fear of persecution or torture, or a fear of return to their home country are referred to USCIS asylum officers to determine whether they have a credible fear of persecution or torture. Individuals determined to have a positive credible fear of persecution or torture are placed into

removal proceedings under INA § 240 by the issuance of a Notice to Appear, and may apply for asylum, withholding of removal or deferral of removal under the INA or the Convention Against Torture as a defense to removal before an immigration judge.

4. Reasonable Fear Screenings

Sections 238(b) and 241(a)(5) of the INA provide for streamlined removal procedures that prohibit certain individuals (i.e., those subject to a final administrative removal order for aggravated felons under section 238(b) or subject to reinstatement of a prior order of exclusion, deportation, or removal under section 241(a)(5) of the INA) from contesting removability before an immigration judge and from seeking any relief from removal. If an individual ordered removed under either section 238(b) or section 241(a)(5) of the INA expresses a fear of return to the country to which he or she has been ordered removed, the case must be referred to a USCIS asylum officer, who determines whether the individual has a reasonable fear of persecution or torture. Individuals found to have a reasonable fear of persecution or torture may seek withholding or deferral of removal before an immigration judge.

Reason for the PIA Update

USCIS Asylum Division primarily relied on legacy Refugees, Asylum, and Parole System (RAPS) and the Asylum Pre-Screening System (APSS) Mainframe to facilitate the adjudication and administration of affirmative asylum, NACARA § 203, credible fear, and reasonable fear cases. The RAPS and APSS Mainframe operating systems have become outdated since they were originally built and have been supplemented by modern technology. USCIS migrated the legacy RAPS and APSS Mainframe operating systems to a cloud-based platform, called Global. This technological advancement does not impact the collection and use of records in Global from the previous legacy system, but does modify the way USCIS stores and maintains affirmative asylum, NACARA § 203, credible fear, and reasonable fear cases records. All RAPS and APSS records were moved into Global.

On December 9, 2010, the Office for Management and Budget (OMB) released a "25 Point Implementation Plan to Reform Federal Information Technology Management," which required the Federal Government to immediately shift to a "Cloud First" policy.[4] The three-part OMB strategy on cloud technology revolves around using commercial cloud technologies when feasible, launching private government clouds, and utilizing regional clouds with state and local governments when appropriate.

[4] 25 Point Implementation Plan to Reform Federal Information Technology Management (December 9, 2010), available at https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf.

When evaluating options for new IT deployments, OMB requires that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. Cloud computing is defined by the National Institute of Standards and Technology (NIST) as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Cloud computing is defined to have several deployment models, each of which provides distinct trade-offs for agencies that are migrating applications to a cloud environment.

USCIS is undergoing a legacy system modernization effort to align with the "Cloud First" policy in order to improve business operations. The USCIS Asylum Division is now primarily served by Global, a cloud-based information technology. Global replaced APSS and RAPS as part of an overall Office of Information Technology initiative to move all mainframe applications to modern cloud-based platforms. As mentioned above, RAPS and APSS were built using a legacy Mainframe system. Global operates on the Amazon Web Services (AWS) cloud platform[5] and combines the functionality of both mainframe systems into one application with a common interface. This migration does not impact the collection and use of records in Global from the previous legacy systems. Historical and existing case data from APSS and RAPS was extracted from the legacy systems and transferred to Global. USCIS requires AWS to segregate Global data from all other data residing in the cloud.

Global is a comprehensive case management tool that enables USCIS Asylum to handle and process applications for asylum pursuant to Section 208 of the INA and applications for suspension of deportation or special rule cancellation of removal pursuant to NACARA § 203. The system also supports USCIS in the screening of individuals in the credible fear and reasonable fear processes. Global continues to capture attorney information, such as name, firm, and address. Each attorney is linked to a system-generated identification code.

AWS is a public cloud designed to meet a wide range of security and privacy requirements (e.g., administrative, operational and technical controls) that are used by USCIS to protect data in accordance with federal security guidelines.[6] AWS is Federal Risk and Authorization Management Program (FedRAMP)-approved and authorized to host PII. FedRAMP is a U.S. Government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud services.

[5] https://marketplace.fedramp.gov/#/product/aws-us-eastwest?status=Compliant&sort=productName.
[6] Public clouds are owned and operated by third-party service providers whereas private clouds are those that are built exclusively for an individual enterprise.

Privacy Impact Analysis

Authorities and Other Requirements

The authority to collect information by the Asylum Division 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 title 8 of the Code of Federal Regulations (CFR). 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 NACARA § 203, in accordance with 8 CFR §§ 240.60 – 240.70, and the maintenance and administration of the credible fear and reasonable fear screening processes, in accordance with 8 CFR §§ 208.30 and 208.31.

The following SORNs cover the collection, maintenance, and use of information by the Asylum Division:

- The Alien File, Index, and National File Tracking System SORN covers the information maintained in the Alien File (A-File),[7] including hardcopy records of asylum applications, NACARA § 203 applications, credible fear screenings, reasonable fear screenings, and supporting documentation;[8]
- The Immigration Biometric and Background Check SORN covers background checks and their results;[9] and
- The Asylum Information and Pre-Screening SORN covers the collection, use, and maintenance of asylum applications, NACARA § 203 applications, credible fear screenings, and reasonable fear screenings.[10]

Global is covered as a minor system under the Digital Innovation Development – Information Technology (DID-IT) Amazon Web Services (AWS) 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 Global, to be reviewed on a monthly basis and sustain its security and privacy posture in order to maintain its Authority to Operate.

[7] USCIS creates an A-File for each individual.
[8] DHS/USCIS-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017).
[9] DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, 83 FR 36950 (July 31, 2018).
[10] DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (Nov. 30, 2015).

Characterization of the Information

This update does not impact the collection of information in Global. USCIS continues to collect and maintain the information outlined in Section 2.0 of the DHS/USCIS/PIA-027(c) Asylum Division, published on July 21, 2017.[11] There are no changes to the forms used by the Asylum Division.

Uses of the Information

This update does not impact the use of information in Global. USCIS uses Global to manage, control, and track the process of affirmative asylum applications, applications for suspension of deportation or special rule cancellation of removal pursuant to NACARA § 203, as well as credible fear and reasonable fear screenings. USCIS uses the information in Global to track case status, facilitate scheduling appointments, issue notices throughout the process, and generate decision documents. USCIS also uses these records to initiate, facilitate, and track security and background check screenings, and to prevent the approval of any benefit prior to the review and completion of all security checks. Finally, USCIS uses these records to generate statistical reports to assist with oversight of production and processing goals.

Notice

This PIA update provides general notice to the public that USCIS retired APSS and RAPS and is using Global as the primary IT case management system for the administration and adjudication of asylum, NACARA § 203, credible fear, and reasonable fear cases. USCIS continues to provide notice to individuals through a Privacy Notice in the associated forms and the associated SORNs.

Data Retention by the project

This update does not impact the retention of information in Global. USCIS stores the physical documents and supplemental documentation in the A-File and processes asylum requests in the respective case management system. The A-File [N1-566-08-11] records are permanent, whether hard copy or electronic, until destroyed, according to the National Archives and Records Administration (NARA) schedule N1-566-08-11. USCIS transfers the A-Files to the custody of NARA 100 years after the individual's date of birth.

NARA approved the retention schedule N1-563-04-06 for RAPS and N1-563-04-07 for APSS. According to both schedules, Master File automated records are maintained for 25 years after the case is closed, then archived for 75 years, and then destroyed. USCIS is planning to consolidate the RAPS and APSS Retention Schedule to cover Global and maintain data for 100 years and then destroy the information to align with the approved A-File schedule. This retention

[11] See DHS/USCIS/PIA-027(c) Asylum Division, available at www.dhs.gov/privacy.

schedule allows the individual to adjust status and naturalize. It also allows USCIS to promptly address any follow-up inquiries (e.g., requests related to security inquiries and Freedom of Information Act/Privacy Act matters).

Information Sharing

This update does not impact the internal and external sharing in Global. USCIS continues to collect and maintain the information outlined in Section 2.0 of the DHS/USCIS/PIA-027(c) Asylum Division, published on July 21, 2017.

Redress

This update does not impact how access, redress, and correction may be sought through USCIS. USCIS continues to provide individuals with access to their information through a Privacy Act or Freedom of Information Act (FOIA) request. Individuals not covered by the Privacy Act or Judicial Redress Act (JRA) still may obtain access to records consistent with FOIA unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. U.S. Citizens and Lawful Permanent Residents may also file a Privacy Act request to access their information. If an individual would like to file a Privacy Act or FOIA request to view his or her USCIS record, the request can be mailed to the following address:

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

Persons not covered by the Privacy Act or JRA are not able to amend their records through FOIA. Should a non-U.S. person find inaccurate information in his or her record received through FOIA, he or she may visit a local USCIS Field Office to identify and amend inaccurate records with evidence.

Auditing and Accountability

USCIS ensures that practices stated in this PIA comply with federal, DHS, and USCIS policies and procedures, including standard operating procedures, orientation and training, rules of behavior, and auditing and accountability procedures.

USCIS employs technical and security controls to preserve the confidentiality, integrity, and availability of the data, which are validated during the security authorization process. Users are required to complete an access request form that is approved by a supervisor before they are granted access. USCIS also implements Role Based Access Controls, which give each user a standard role and a standard set of permissions to prevent the user from accessing anything outside their assigned role. These technical and security controls limit access to USCIS users and mitigates privacy risks associated with unauthorized access and disclosure to non-USCIS users.

Further DHS security specifications also require auditing capabilities that log the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify information by user identification, network terminal identification, date, time, and data accessed. All USCIS systems employ auditing measures and technical safeguards to prevent the misuse of data.

In addition, all contracted cloud service providers must also follow DHS privacy and security policy requirements. Before using AWS, USCIS verifies through an independent risk assessment that AWS met all DHS and USCIS privacy and security policy requirements. Further, all cloud-based systems and service providers are added to the USCIS Federal Information Security Modernization Act (FISMA) inventory and are required to undergo a complete security authorization review to ensure security and privacy compliance. As part of this process, the DHS Senior Agency Official for Privacy reviews all FedRAMP cloud service providers for privacy compliance and privacy controls assessments as part of the privacy compliance review process.

Privacy Risk: There is a risk that Global records can be accessed by unauthorized personnel since Global now resides in AWS, a public cloud.

Mitigation: This risk is mitigated. Although Global operates in a public cloud, it is separated from other public cloud customers. Global operates in a Virtual Private Cloud, which is a private component to the public cloud. USCIS controls access to the systems within the cloud, not AWS.

Responsible Official

Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
Department of Homeland Security

Approval Signature

[Original signed and on file at the DHS Privacy Office]

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security