



**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) § 203² 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 platform⁵ 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