Privacy Impact Assessment

for the

Pangaea:

Pangaea Text

DHS Reference No. DHS/USCIS/PIA-085

January 6, 2021

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Citizenship and Immigration Services (USCIS) uses Pangaea, a suite of customized data-driven applications that provide actionable intelligence for USCIS to make informed operational decisions. The first application that USCIS plans to use is Pangaea Text, a secure web-based system, to assist in safeguarding the integrity of the asylum program by identifying fraud, national security, and public safety concerns. USCIS is issuing this Privacy Impact Assessment (PIA) to discuss the risks and mitigations associated with the use of Pangaea Text. As USCIS continues to use additional tools within the Pangaea suite, USCIS will issue updates to this PIA.

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,[1] Congress charged USCIS with administering the asylum program. USCIS, through its Asylum Division within the Refugee, Asylum & International Operations Directorate (RAIO), 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 Title 8 of the Code of Federal Regulations (C.F.R.), 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, and related threshold and fear assessments as promulgated by federal rules and implementing policies.

Affirmative Asylum

Every year individuals come to the United States seeking asylum 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. An individual can obtain asylum in the United States in one of two ways, through the affirmative process before USCIS or through the defensive process before an immigration judge (IJ) in the U.S. Department of Justice's Executive Office for Immigration Review (EOIR).[3] To obtain affirmative asylum, the individual must be physically present in the United States and meet the statutory requirements. An individual

[1] 6 U.S.C § 2711 *et seq*.
[2] Pub. L. No. 105-100, 111 Stat. 2193 (November 19, 1997), amended by Pub. L. No. 105-139, 111 Stat. 2644 (December 2, 1997).
[3] Immigration Judges are adjudicators within the U.S. 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.

may include as derivatives on his or her asylum application, his or her spouse and/or unmarried children under 21 years of age who currently reside in the United States.

USCIS is responsible for the administration and adjudication of the affirmative asylum process. Individuals granted asylum status, as well as their spouse or unmarried children under 21 years of age who are in the United States and are included on the application as derivatives:

- Possess this status indefinitely;
- May work in the United States; and
- May apply for permanent residence after one year.

Individuals granted asylum status may also request derivative status for their spouse or unmarried children under 21 years of age within two years of the grant of asylum status, if these family members were not initially included as derivatives at the time of the grant of asylum.

Generally, 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*,[4] with USCIS.[5] Form I-589 may be submitted to USCIS by either the asylum applicant or the applicant's attorney or representative. Form I-589 collects biographic information including:

- Name;
- Alien Registration Number (A-Number);
- U.S. and foreign addresses;
- Phone number;
- Education and employment history; and
- Criminal history.

An applicant is required to complete Part B of the application, which asks for detailed and specific information about his or her asylum claim, including details about specific events supporting his or her fear of persecution on account of a protected ground (race, religion, nationality, political opinion, or membership in a particular social group), evidence of relevant country conditions, and the specific facts which the individual is relying on to support his or her claim. Using a narrative format, Part B of the I-589 seeks to compile dates, places, and descriptions about each event or action relevant to the applicant's claim. Written narratives may include information about the

[4] The Form I-589 is available at www.uscis.gov/forms.
[5] Withholding 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.

individual's background, to include family history, education history, work history, social life history, and political life history. Finally, the applicant is strongly urged to submit an optional supplementary written statement to further explain the claim discussed in Part B.

USCIS Asylum Officers review Form I-589 and supporting evidence submitted to USCIS by the applicant. Asylum Officers verify the information provided on the form; conduct biographic and biometric based background and identity checks by querying USCIS, DHS, and external systems; and interview affirmative asylum applicants within the jurisdiction of USCIS prior to the full adjudication of their asylum request. During the course of the adjudication process, if the asylum applicant fails to submit evidence or provides insufficient evidence to establish eligibility, USCIS may issue a Request for Evidence (RFE).[6] Asylum Officers make asylum adjudication decisions based on the totality of the evidence (e.g., documentary evidence, interview testimony, background and identity checks, and Fraud Detection and National Security (FDNS) review (as described below)) obtained through the adjudicative process. USCIS relies on multiple sources to make an adjudication decision.

A full description of the Asylum process can be found in the DHS/USCIS/PIA-027 Asylum Division.[7]

FDNS Administrative Investigations

In furtherance of USCIS' mission to safeguard the integrity of the nation's lawful immigration system, the FDNS Directorate leads agency efforts to detect, deter, and combat fraud, national security, and public safety threats, and maximizes law enforcement and Intelligence Community (IC) partnerships. FDNS personnel are embedded in each Asylum Office. Asylum Officers refer an asylum application to their local FDNS team when they have identified concerns related to national security, fraud, and/or public safety during the course of adjudication.[8]

FDNS Immigration Officers support agency adjudications by gathering, compiling, and analyzing information that an adjudicator can consider when rendering a final decision on an immigration benefit request. FDNS Immigration Officers may conduct administrative investigations by reviewing, inspecting, collating, and comparing information from documents submitted by asylum applicants to identify patterns, trends, and indicators of fraud, national security, and/or public safety concerns. If FDNS investigations reveal criminal activity, or national

[6] USCIS uses an RFE when an application lacks required documentation or when the adjudicator needs additional evidence to determine an applicant's eligibility for the benefit sought. The request will indicate what evidence or information USCIS needs to fully evaluate the application or petition under review.
[7] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE USCIS ASYLUM DIVISION, DHS/USCIS/PIA-027 (2017 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[8] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE FRAUD DETECTION AND NATIONAL SECURITY DIRECTORATE, DHS/USCIS/PIA-013-01 (2019 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

security concerns, FDNS Immigration Officers refer their findings to law enforcement or intelligence community agencies, as appropriate.

Pangaea Text

While applicants will soon have the option to file asylum applications electronically, currently, asylum applications and supporting documents are submitted in a paper format to USCIS and retained by USCIS in physical Alien Files (A-Files). Consequently, Asylum Officers and FDNS Immigration Officers review a large volume of paper documents in order to identify information relevant to issues of asylum eligibility or fraud, national security, and/or public safety. The existing process requires USCIS officers to visually review pages of the application packet and to navigate through a paper file, potentially multiple times throughout the course of the adjudication.

To address the inefficiencies arising from time-intensive manual reviews, USCIS developed Pangaea Text, a secure web-based system, to enhance the document review process by Asylum Officers and FDNS Immigration Officers. Pangaea Text applies rules and algorithms to detect patterns that could constitute indicators of fraud, national security, and/or public safety concerns across digitized asylum applications and supplementary written statements. Pangaea Text transforms unstructured text documents into usable, structured data. Pangaea Text does *not* perform system-automated adjudications. All results are reviewed by USCIS personnel.

Pangaea analyzes narrative aspects of Form I-589 - including Part B, the supplementary written statement, and any certificate of translation pertaining to that written statement. Applicants often submit their written statements in their native language and as an English translation. Pangaea Text stores the English translation and any certificate of translation, which is typically appended to the end of the written statement or attached as a separate document. Pangaea Text does not ingest or store the native language version at this time. Pangaea Text has the capability to locate patterns that are relevant to asylum adjudications and administrative investigations.

All asylum applications, including those pending in the existing asylum backlog, are planned to eventually be ingested into Pangaea Text. USCIS ingests asylum application information through direct system interconnections with other systems, such as the Immigrant Visa Content Service (IVCS).[9] From these systems, Pangaea Text receives content extracted from Form I-589, including the narrative sections, such as Part B, and the supplementary written statement. The digital copies of this content are produced by scanning physical paper records at capture facilities, including the USCIS National Records Center, as well as at other USCIS facilities, using scanning devices. Pangaea Text captures information from Form I-589, the supplementary written

[9] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE INTEGRATED DIGITIZATION DOCUMENT MANAGEMENT PROGRAM (IDDMP), DHS/USCIS/PIA-003(b) (2007 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

statement, and the translation certificate, if applicable. Global[10] and the Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR)[11] provide Pangaea Text with additional and/or updated background, identity, and biographic information for applicants and dependents including address and/or attorney changes. USCIS is planning to introduce electronic filing of Form I-589 in the near future. Once USCIS begins accepting electronic Form I-589s, USCIS will expand the interconnection with Pangaea Text to Global and myUSCIS[12] and will continue to leverage the information from Global to receive the I-589 application and supplementary evidence. Additionally, Pangaea Text will ingest scanned and uploaded paper applications via a direct connection with Global. USCIS will continue to use Pangaea Text to review both paper and electronically submitted applications.

Using the ingested application and supplementary information, Pangaea Text applies rules and algorithms to sort through the information to identify patterns that may indicate potential fraud, national security, and/or public safety concerns. While Pangaea Text retains the entirety of the Form I-589, it only analyzes the narrative portions (e.g., Part B and supplementary written statements).

The rules and algorithms are used to create the automated pattern identification. The results of the automated pattern identification are displayed as a report to FDNS Immigration Officers through a web-based user interface. The report displays a copy of the application where portions of the application have been highlighted to indicate the algorithms and rules-identified patterns. If the FDNS Immigration Officer determines through manual review that a pattern identified through Pangaea Text may relate to a potential indicator of fraud, national security, and/or public safety concerns as flagged by Pangaea Text, after a thorough review, the FDNS Immigration Officer may prepare a Statement of Findings (SOF) or other standardized FDNS work product and include therein the relevant Pangaea Text information. SOFs and other FDNS documents are developed by FDNS Immigration Officers and are used to document their review and findings. Such a document may be considered by an adjudicator who will determine whether the individual is eligible for an immigration benefit. These FDNS documents are stored in the FDNS-Data System

[10] *See supra* note 6.
[11] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE CITIZENSHIP AND IMMIGRATIONS SERVICES CENTRALIZED OPERATIONAL REPOSITORY (eCISCOR), DHS/USCIS/PIA-023 (2009 and subsequent updates) and, DHS/USCIS/PIA-027 (2017 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[12] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR MYUSCIS, DHS/USCIS/PIA-064 (2019) and, DHS/USCIS/PIA-027 (2017 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

(DS)[13] and are provided to Asylum adjudications personnel to provide them with information they may consider when making an asylum decision.

In addition to receiving SOFs or other FDNS documents from FDNS Immigration Officers, Asylum Officers have direct access to Pangaea Text. Asylum Officers may query the system using the individual's Alien Number (A-Number), to display the report produced for the respective application. The Asylum Officer may also confer with FDNS personnel, who will be able to review the results and provide more information and context regarding the system's findings, as appropriate. The Asylum Officer determines if a pattern identified through Pangaea Text and/or documented in an FDNS work product is relevant to the adjudication of the asylum application. When the information is relevant, the information may be used in evaluating the applicant's eligibility for asylum. The Asylum Officer's adjudication is documented and retained in the A-File.[14]

Importantly, Pangaea Text does *not* perform system-automated adjudications or make FDNS determinations. Instead, Pangaea Text automatically identifies patterns and potential indicators of fraud, national security, and/or public safety concerns that may require further review by an FDNS Immigration Officer, who has the authority to review that information and, if appropriate, make a determination about the presence of fraud, national security, and/or public safety concerns, which may result in an administrative investigation. It is only an Asylum Officer who is responsible for evaluating how or if that evidence impacts asylum eligibility.

In addition to the report Pangaea Text creates, Pangaea Text information is also replicated in eCISCOR for reporting and statistical analysis, in eCISCOR's reporting tools such as the Standard Management Analysis Reporting Tool (SMART).[15] eCISCOR-generated reports contain text extracted from digitized copies of Form I-589 and the supplementary written statement as well as the results of the automated pattern identification to view in a readable form.

The USCIS Office of Privacy will work collaboratively with RAIO on all future rule/algorithm development efforts to ensure a comprehensive privacy analysis of any updates is completed, including the mitigation of any resulting privacy risks.

---

[13] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE FRAUD DETECTION AND NATIONAL SECURITY-DATA SYSTEM, DHS/USCIS/PIA-013 (2008 and subsequent updates) *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[14] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 Fed. Reg. 43556 (September 18, 2017), *available at* https://www.dhs.gov/system-records-notices-sorns.

[15] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE STANDARD MANAGEMENT ANALYSIS REPORTING TOOL, DHS/USCIS/PIA-050 (2013), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

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 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 C.F.R. As set forth in Section 451(b) of the Homeland Security Act of 2002, Public Law 107-296,[16] 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 C.F.R. Part 208.

8 C.F.R. Part 208.3(a) requires that an asylum applicant file the Form I-589, together with any additional supporting evidence, in accordance with the instructions on the form. 8 C.F.R. Part 208.4(b) also requires an applicant to file the Form I-589 in accordance with the form's instructions. 8 C.F.R. Part 208.9(e) requires the Asylum Officer to consider the asylum application, as well as any evidence submitted by the applicant. In addition, 8 C.F.R. 208.9(f) states that the asylum application and all information provided by the applicant, in addition to any other information specific to the applicant's case and considered by the officer, and any comments submitted by the Department of State, shall comprise the record.

Furthermore, the INA, 8 U.S.C. § 1101, et seq., provides the legal authority to collect information used for the adjudication of immigration benefits. The Secretary of Homeland Security in Homeland Security Delegation No. 0150.1, delegated USCIS the authority to investigate alleged civil and criminal violations of the immigration laws, including alleged fraud with respect to applications or determinations within the U.S. Bureau of Citizenship and Immigration Services (BCIS) [predecessor to USCIS], and to make recommendations for prosecutions or other appropriate action when deemed advisable.

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 for Pangaea Text:

- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System covers the information maintained in the A-File, including hardcopy records of asylum applications and supporting documentation;[17]

[16] *See supra* note 1.
[17] *See supra* note 12.

- DHS/USCIS-010 Asylum Information and Pre-Screening covers the collection, use, and maintenance of the affirmative asylum applications that will be analyzed using Pangaea Text;[18] and
- DHS/USCIS-006 Fraud Detection and National Security Records covers the information collected, maintained, used and generated by FDNS as part of the FDNS mission.[19]

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

Pangaea Text is a minor application that is currently undergoing the Authority to Operate (ATO) review process under FDNS-DS. Pangaea Text is within the FDNS-DS accreditation boundary but is not directly connected to FDNS-DS. FDNS-DS was approved for entrance into the DHS Ongoing Authorization Program on August 26, 2014. Ongoing Authorization requires FDNS-DS and the systems within its boundary to be reviewed on a monthly basis and to maintain its security and privacy posture in order to retain its ATO. The security controls and organizational risks are assessed and analyzed (that vary by security control) to support risk-based security decisions. FDNS-DS and the systems within its boundary also undergo regular security audits to assess security compliance.

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

The information contained in Pangaea Text is considered non-record[20] copies and deleted when no longer operationally needed. Information yielded by Pangaea Text will be used by FDNS Immigration Officers and Asylum Officers, as appropriate. Therefore, Pangaea Text information may be saved in FDNS-DS and the individual's A-File, respectively. FDNS retains information in FDNS-DS for 15 years from the date of the last interaction between FDNS personnel and the individual for records maintained in FDNS-DS and its associated subsystems [N1-566-08-18].[21] USCIS retains A-File records for 100 years from the individual's date of birth, and then transfers

[18] *See* DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 Fed. Reg. 74781 (November 30, 2015), *available at* https://www.dhs.gov/system-records-notices-sorns.
[19] *See* DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 Fed. Reg. 47411 (August 8, 2010), *available at* https://www.dhs.gov/system-records-notices-sorns.
[20] Information contained within Pangaea Text is considered a non-record copy as it is just a scanned copy of the I-589. The original I-589 and supporting affidavit that are placed in the A-File are considered the "record."
[21] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER N1-566-08-18, U.S. DEPARTMENT OF HOMELAND SECURITY, FRAUD DETECTION AND NATIONAL SECURITY (FDNS) DATA SYSTEM (2008), *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0566/n1-566-08-018_sf115.pdf.

the records to NARA [N1-566-08-11].[22]

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.

Pangaea Text is not subject to the Paperwork Reduction Act requirements, as Pangaea Text does not collect information directly from an individual. However, Pangaea Text stores information extracted from digitized copies of Form I-589, *Application for Asylum and for Withholding of Removal* (OMB No. 1615-0067), which is covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

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

Pangaea Text stores information extracted from a digital copy of Form I-589, *Application for Asylum and for Withholding of Removal*, and the supplemental written statement submitted in support of Form I-589. Appendix A to this PIA lists data elements that are included on the Form I-589. Pangaea Text retains the entirety of the Form I-589, but only analyzes the narrative portions of the form and the supplementary written statement. These statements often include personally identifiable information (PII) and other sensitive information, such as:

- A-Number;
- Name;
- Passport number;
- Address;
- Country of birth;
- Religion; and
- Ethnicity.

Pangaea Text has a connection to Global, the IT case management system for programs administered by the Asylum Division, and eCISCOR, a USCIS data repository that retrieves,

[22] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER N1-566-08-11, U.S. DEPARTMENT OF HOMELAND SECURITY, ALIEN FILES (A-FILES) (2009), *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0566/n1-566-08-011_sf115.pdf.

stores, and sends information to other USCIS systems. Through a connection to these systems, Pangaea Text receives additional background, identity, and biographic information of applicants and dependents included on the application for asylum, such as:

- First name;
- Last name;
- Address;
- Country of birth; and
- Attorney information.

Pangaea Text displays such information to reduce the need for officers to access multiple systems in the course of assessing an indicator or pattern identified by Pangaea Text. Global stores a record that Pangaea Text has ingested a given applicant's Form I-589 and supplementary written statement, if available. USCIS may also create additional reports using eCISCOR's reporting tools,[23] such as SMART.

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

Pangaea Text stores information extracted from Form I-589, *Application for Asylum and for Withholding of Removal*, and the supplemental written statement submitted by the applicant or legal representative. Global and eCISCOR provide Pangaea Text with additional background, identity, and biographic information.

Pangaea Text receives this information to reduce the need for officers to access multiple systems in the course of using Pangaea Text.

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

This project does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

FDNS Immigration Officers and Asylum Officers may initiate queries in Pangaea Text, review the results, and then validate their findings from the digitized data by reviewing the source paper-based or electronic documentation. If Pangaea Text detects a relevant pattern or indicator, an Asylum Officer and/or FDNS Immigration Officer will perform a manual review to evaluate

[23] USCIS is publishing a separate PIA to analyze the privacy risks and mitigations associated with eCISCOR's reporting tools.

whether the system-generated information can be used to draw an adjudicative or investigatory determination. This review includes an inspection of source documents from which the information was extracted, when applicable. FDNS will only include Pangaea Text information in a SOF or other FDNS document if it is determined to be relevant to such a fraud, national security, and/or public safety indicator or concern or would potentially impact eligibility. FDNS requires supervisory review of all fraud findings on asylum applications. The FDNS Supervisory Immigration Officer reviews the entirety of the record to ensure the evidence discovered by FDNS or submitted by the applicant supports the finding. The FDNS Supervisory Immigration Officer also reviews the FDNS SOF for completeness and accuracy.

Additionally, the Asylum Division has a Quality Assurance Branch that provides guidance to adjudicators on use of information from Pangaea Text during the asylum adjudication process. The Quality Assurance Branch performs reviews of certain asylum applications that involve complex or sensitive issues.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that Pangaea Text will misrecognize text within Form I-589 or the supplemental statement, resulting in data inaccuracies.

Mitigation: This risk is partially mitigated. For paper-based Form I-589s and supplementary written statements, the data within Pangaea Text is obtained using optical character recognition (OCR) of digitized asylum documents. OCR enables the recognition of text (letters, numbers, and symbols) from images of physical documents. OCR has the potential to misrecognize characters, resulting in an inaccurate representation of the digitized text relative to the physical copy. For example, the letter "B" may be misrecognized as the number "3" during the OCR process. USCIS mitigates this risk by using OCR software that produces a score indicating the confidence that the text was accurately recognized. Users are notified in the Pangaea Text graphical interface when the OCR confidence falls below 90%, as the graphical interface will display a warning banner stating, "Scanned Text May Contain Errors" over a specific line or section of text where the OCR confidence is low. In these circumstances, officers are trained to reference the source documents. In addition, officers must manually review source documents when using information from Pangaea Text to produce SOFs and other work products.

This risk will be further mitigated when Pangaea Text begins to ingest and store information extracted from electronically filed Form I-589s and written statements, filed through e-processing. An electronically filed Form I-589 would not need to undergo the OCR process, as Pangaea Text will receive the application in a digital format directly from the source system, Global or myUSCIS.

Privacy Risk: Pangaea Text may indicate a pattern exists that may not actually relate to a fraud, national security, or public safety indicator or concern.

Mitigation: This risk is mitigated. Asylum Officers and FDNS Immigration Officers with access to Pangaea Text are trained on all relevant policies, procedures, laws, and regulations, and understand that Pangaea Text is *not* an automated decision-making tool, but instead a software program to assist officers in identifying patterns of potential fraud, national security, and/or public safety indicators or concerns. The Pangaea Text system determines whether a pattern or indicator exists but does not analyze whether that pattern or indicator constitutes a fraud, national security, and/or public safety indicator or concern; only an FDNS Immigration Officer can make such a determination, and only an Asylum Officer can determine how, if at all, the indicator or concern impacts asylum eligibility. USCIS officers are also trained in developing lines of questioning and requests for evidence that may help determine the relevancy of Pangaea Text findings. Finally, USCIS officers are trained to reference the source documents prior to any adjudication decision being made.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Pangaea Text uses data elements extracted from a digital copy of Form I-589, supplemental written statements submitted in support of Form I-589, and other USCIS systems. This information is provided directly by the applicant or their representative to USCIS in association with the applicant's immigration request before the agency. Information in Pangaea Text is made available to authorized Asylum Officers and FDNS Immigration Officers. Officers may initiate queries, review the results, and validate their findings in the digitized data by reviewing the source documentation. If Pangaea Text identifies a pattern within the data, a trained officer will perform a manual review to evaluate whether the system-generated information from Pangaea Text can be used to draw an adjudicative or investigatory determination or if the pattern is relevant to fraud, national security, or public safety. This review includes an inspection of the source documents from which the information was extracted. FDNS will only include Pangaea Text information in a SOF or other FDNS work product if it is determined to actually be relevant to a fraud, national security, and/or public safety indicator or concern. An Asylum Officer will evaluate the report in Pangaea Text, as well as any additional information provided by FDNS, and will determine whether the report and any available FDNS findings impact eligibility for the benefit sought.

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.

Pangaea Text will produce a result indicating whether or not there is a pattern associated with a possible fraud, national security, and/or public safety risk in data derived from asylum applications and supplementary supporting statements submitted to USCIS. These results will be maintained in Pangaea Text for review by an Asylum Officer and FDNS Immigration Officer. The FDNS Immigration Officer will review the results to determine if Pangaea Text has in fact discovered a fraud, national security, and/or public safety indicator or concern and subsequently will make a determination as to whether it requires follow-up action according to standard operating procedures (SOP). An Asylum Officer will also evaluate the results in Pangaea Text, as well as any additional information provided by FDNS, and will determine whether the results and any available FDNS findings impact eligibility for the benefit sought. The FDNS Immigration Officer may include manually reviewed Pangaea Text information in a SOF, or other FDNS product, which may be provided to adjudications personnel and stored in the A-File in accordance with FDNS procedures.

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

Pangaea Text is not accessible outside of USCIS. However, manually reviewed information derived from queries in Pangaea Text may be shared with other DHS components, such as U.S. Immigration and Customs Enforcement (ICE), for investigatory and immigration court functions, and with other USCIS directorates for adjudicative functions. Law enforcement agencies may receive information derived from Pangaea Text on a case-by-case basis, if warranted, in connection with an official criminal or national security investigation. The sharing of information contained within asylum applications is described in DHS/USCIS/PIA-027 USCIS Asylum Division.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of unauthorized access to Pangaea Text.

Mitigation: This risk is mitigated. USCIS protects Pangaea Text from unauthorized access through administrative, physical, and technical safeguards that include restricting access to authorized personnel who have a valid need-to-know to access the information in Pangaea Text. RAIO and FDNS management personnel determine who is permitted to access the system. Access to Pangaea Text is managed in accordance with existing USCIS procedures. All access requests are routed through the employee's management to the Pangaea Text product owner. Asylum-

related data is governed by strict regulatory confidentiality provisions outlined in 8 C.F.R. Part 208.6, "Disclosure to Third Parties" and covered by DHS/USCIS/PIA-027 USCIS Asylum Division. All USCIS personnel handling asylum-related data are trained in disclosure policies.

Privacy Risk: There is a risk that Asylum Officers will rely on inaccurate information produced by Pangaea Text to make an asylum determination.

Mitigation: This risk is mitigated. The reports produced by Pangaea Text and the analysis of these reports by FDNS Immigration Officers and Asylum Officers inform, but do not solely determine, the outcome of an affirmative asylum application. It is the responsibility of the Asylum Officer to evaluate the substance and assess the reliability of the additional information uncovered by Pangaea Text, in conjunction with other information available to the Asylum Officer in determining whether to approve or deny an application. Asylum Officers make asylum adjudication decisions based on the totality of the evidence (e.g., documentary evidence, interview testimony, background and identity checks, and FDNS administrative investigations) obtained through the adjudicative process. USCIS relies on multiple sources of information to make an adjudication decision. Thus, the Pangaea Text results will inform the affirmative asylum adjudication, but will not be the sole basis for the adjudicative outcome.

Section 4.0 Notice

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

USCIS provides general notice to individuals through a Privacy Notice on the instructions of the Form I-589. The form asks applicants to provide information that is relevant to their eligibility for asylum, including information about criminal acts, immigration violations, and other unlawful activity. The applicant is required to sign the form certifying that he or she authorizes USCIS to release any information received from the applicant, as needed, to determine eligibility for benefits and, when necessary, for the administration and enforcement of U.S. immigration laws.

USCIS also publishes information about the asylum process on the USCIS website.[24] This webpage provides details as to what the applicant can expect during the review and adjudication process. Individuals also receive notice through DHS/USCIS/PIA-027 USCIS Asylum Division.

Individuals receive notice about Pangaea specifically through this PIA.

Individuals also receive general notice through the following SORNs:

[24] *See* https://www.uscis.gov/humanitarian/refugees-asylum/asylum/affirmative-asylum-process.

- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System;[25]
- DHS/USCIS-010 Asylum Information and Pre-Screening;[26] and
- DHS/USCIS-006 Fraud Detection and National Security Records.[27]

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

The instructions for the Form I-589 contain a Privacy Notice. The 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, a statement that the information that the applicant provides is voluntary, and the consequences of declining to provide the requested information to USCIS. To determine whether an individual is eligible for asylum, he or she must complete the Form I-589 and may choose to provide supplemental evidence where appropriate. By signing the Form I-589, the applicant affirms that they authorize the release of any information from their immigration record that USCIS needs to determine their eligibility for asylum. USCIS must assess this information to make an adjudication decision to grant or deny an immigration benefit and to safeguard the integrity of the program by identifying indicators of fraud, national security, and public safety concerns.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that applicants may not be aware that their information is evaluated using Pangaea Text.

Mitigation: This risk is partially mitigated. While USCIS generally provides an overview of the application review process on the USCIS website and other PIAs, USCIS does not provide specific details of the review process or the use of Pangaea Text. USCIS is providing notice of Pangaea Text through the publication of this PIA, since the use of this tool involves PII.

Section 5.0 Data Retention by the Project

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

The information contained in Pangaea Text is considered non-record copies and deleted when no longer operationally needed. Information yielded by Pangaea Text will be used by FDNS Immigration Officers and Asylum Officers, as appropriate. Therefore, Pangaea Text information may be saved in FDNS-DS and in the individual's A-File, respectively. FDNS retains information in FDNS-DS for 15 years from the date of the last interaction with the individual for records

[25] *See supra* note 12.
[26] *See supra* note 15.
[27] *See supra* note 16.

maintained in FDNS-DS and its associated subsystems [N1-566-08-18]. USCIS retains A-File records for 100 years from the individual's date of birth, and then transfers the records to NARA [N1-566-08-11].

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information will be maintained for longer than necessary.

Mitigation: This risk is mitigated. All data retained in Pangaea Text is considered a non-record copy and destroyed when no longer operationally needed. Results yielded by Pangaea Text that are used for FDNS mission-related purposes or by an Asylum Officer for adjudicative purposes are stored in FDNS-DS and the A-File in accordance with those respective retention periods.

Section 6.0 Information Sharing

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

USCIS is not granting external entities access to Pangaea Text as part of regular agency operations. However, manually reviewed Pangaea Text information may be shared with other DHS and law enforcement entities for removal proceedings or law enforcement purposes. USCIS may share asylum information with the intelligence community, consistent with DHS's mission to prevent and deter terrorist attacks and to ensure that immigration benefits are not granted to individuals who pose a threat to national security. Information sharing of asylum data is discussed in DHS/USCIS/PIA-027 USCIS Asylum Division. If information is shared with non-asylum office government personnel within USCIS, DHS, the U.S. Department of Justice, or other government entities, all applicable rules, laws, policies, and SOPs are followed. The information derived from Pangaea Text may be presented in a USCIS work product authored by subject matter experts, such as FDNS Immigration Officers or Asylum Officers, who contextualize their findings to ensure that it is accurately interpreted by external audiences.

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

The DHS/USCIS/PIA-027(c) Asylum Division provides an explanation of external sharing and how the sharing is compatible with the purpose for which the information was originally requested.

The routine uses of the respective SORNs that cover asylum data identify the manner in which it may be shared outside of DHS. For example, routine use G in the DHS/USCIS-010

Asylum Information and Pre-Screening SORN[28] states that information may be shared "To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure 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." Routine use H states that information may be shared "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 function or functions and the information received will be used for the authorized purpose for which it is requested."

6.3 Does the project place limitations on re-dissemination?

Pangaea Text is not accessible externally and therefore does not place limits on re-dissemination. However, as noted above, any work products that USCIS personnel create that may be shared externally are protected by 8 C.F.R. § 208.6 "Disclosures to Third Parties," discussed more fully in DHS/USCIS/PIA-027 USCIS Asylum Division. Any re-dissemination is overseen by USCIS and memorialized by USCIS and the receiving entity in a Memoranda of Understanding/Agreement (MOU/A) entered into prior to the systemic sharing of information with an external organization. The disclosure of information protected by 8 C.F.R § 208.6 is only permissible if it falls within one of the exceptions provided for in the regulation. USCIS disseminates only information from Pangaea Text that has been reviewed and evaluated by an FDNS Immigration Officer.

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

Any dissemination of manually reviewed Pangaea Text information to non-USCIS partners for law enforcement purposes is recorded in FDNS-DS and may be noted in the A-File or in the system logs of other USCIS systems, in accordance with policy and procedure.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information viewable in Pangaea Text may be disseminated by USCIS personnel inappropriately.

[28] *See supra* note 15.

Mitigation: This risk is mitigated. All USCIS personnel with access to Pangaea Text receive training on the use and release of information and are required to follow applicable SOPs, rules, laws, and policies, including strict regulatory confidentiality provisions contained in 8 C.F.R. Part 208.6, "Disclosure to Third Parties". Additionally, all employees with access to protected asylum information in USCIS systems must read and sign an acknowledgement of confidentiality obligations concerning asylum-related information. The confidentiality obligations acknowledgment form contains the text of 8 C.F.R. Part 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 USCIS systems.

Privacy Risk: There is a risk that data shared by USCIS with external partners will be used beyond the original purpose of collection to determine eligibility for asylum.

Mitigation: This risk is partially mitigated. USCIS employs practices and procedures to ensure that data is shared with external agencies pursuant to one of the exceptions provided for in 8 C.F.R. § 208.6 and is compatible with the applicable SORNs. All prospective information handlers must be authorized to access the information and be made aware of the fact that the information is protected by the confidentiality provisions of 8 C.F.R. § 208.6. 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.

FDNS maintains a record of each disclosure of FDNS information made to every agency consistent with a routine use and with whom it has an information sharing agreement. Otherwise, FDNS does not share its information. A record is kept of each disclosure, including the date the disclosure was made, the agency to which the information was provided, the purpose of the disclosure, and a description of the data provided.

The electronic sharing of data with external agencies is conducted over government secure networks and utilizing secure protocols such as passwords and/or encryption to ensure the security of the data. All personnel within the receiving agency and its components are trained on the appropriate use and safeguarding of data. In addition, each external agency with whom the information is shared has policies and procedures in place to ensure there is no unauthorized dissemination of the information provided by FDNS. Any disclosure must be compatible with the purpose for which the information was originally collected, and pursuant to one of the exceptions provided for in 8 C.F.R. § 208.6.

Risks are further mitigated by provisions set forth in MOAs or MOUs with federal and foreign government agencies. Finally, U.S. Government employees and contractors must undergo annual privacy and security awareness training.

Section 7.0 Redress

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

An individual may gain access to his or her USCIS records by filing a Privacy Act (PA) or Freedom of Information (FOIA) request. Only U.S. citizens, lawful permanent residents, and individuals covered by the Judicial Redress Act of 2015 (JRA) may file a Privacy Act request. Any person, regardless of immigration status, may file a FOIA request. If an individual would like to file a Privacy Act or FOIA request to view his or her USCIS record, he or she may mail the request to the below address or submit a request online at https://www.uscis.gov/records/request-records-through-the-freedom-of-information-act-or-privacy-act:

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

National Records Center requests for access to records must be in writing. Such requests may be submitted by mail or in person. If a request for access is made by mail, the envelope and letter must be clearly marked "Privacy Act Request" to ensure proper and expeditious processing. The requester should provide his or her full name, date and place of birth, and verification of identity in accordance with DHS regulations governing Privacy Act requests (found at 6 C.F.R. Part 5.21), and any other identifying information that may be of assistance in locating the record.

However, because Pangaea Text contains sensitive information related to possible immigration benefit fraud, national security, and/or public safety indicators and/or concerns that may compromise an ongoing investigation, the requested information may be exempt from the notification, access, and amendment provisions of the Privacy Act of 1974, pursuant to 5 U.S.C. § 552a(k)(2).

Notwithstanding the applicable exemptions, USCIS reviews all such requests on a case-by-case basis. When such a request is made, and access would not appear to interfere with or adversely affect the national or homeland security of the U.S. or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of USCIS, and in accordance with procedures and points of contact published in the applicable SORNs.

Additional information about PA/FOIA requests for USCIS records can be found at http://www.uscis.gov.

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

Information in Pangaea is not collected directly from the individual; however, the data is derived from the Form I-589 and affidavits submitted by the individual. Corrections to the data accessed by Pangaea Text from Global and eCISCOR would need to be made in the source systems. In the event inaccuracies are identified, the information in Pangaea Text will be updated.

U.S. citizens, lawful permanent residents, and individuals covered by the JRA are afforded the ability to correct information by filing a Privacy Act Amendment as discussed in Section 7.1. The requestor should clearly and concisely state the information being contested, the reason for contesting or amending it, the proposed amendment, and any evidence of the correct information. 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 also able to amend their records. If a person finds 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 on USCIS forms, the USCIS website, this PIA, and the applicable SORNs identified in Section 1.2.

7.4 Privacy Impact Analysis: Related to Redress

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

Section 8.0 Auditing and Accountability

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

Access to Pangaea Text is granted to FDNS and Asylum personnel who receive supervisory approval and approval from the product owner, and who have undergone required training. In accordance with DHS security guidelines, Pangaea Text has auditing capabilities that log user activities. Pangaea Text tracks all user actions via security audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. Pangaea Text

employs technical safeguards to prevent the misuse of data. Many users have legitimate job duties that require them to design, develop, and optimize the system. These users perform this work under supervisory oversight. USCIS requires each employee to undergo an annual security awareness training that addresses his or her duties and responsibilities to protect the integrity of the information. When employment at USCIS is terminated or an employee's responsibilities no longer require access to Pangaea Text, access privileges are removed.

Furthermore, Pangaea Text is housed in the FedRAMP-approved Amazon Web Services (AWS) cloud environment, at a moderate confidentiality that allows USCIS to host PII.[29] AWS U.S. East/West is a multi-tenant public cloud designed to meet a wide range of regulatory requirements, including government compliance and security requirements.[30] FedRAMP is a U.S. Government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud services. USCIS is responsible for all PII associated with the Pangaea Text system, whether on a USCIS infrastructure or on a vendor's infrastructure, and it therefore imposes strict requirements on vendors for safeguarding PII data. This includes adherence to the DHS 4300A Sensitive Systems Handbook,[31] which provides implementation criteria for the rigorous requirements mandated by DHS's Information Security Program.

The USCIS Office of Privacy will work collaboratively with RAIO on all future rule/algorithm development efforts to ensure a comprehensive privacy analysis of any updates is completed, including the mitigation of any resulting privacy risks.

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

All USCIS employees receive the required annual Computer Security Awareness training and Privacy Act 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. USCIS employees who have access to Pangaea Text are trained on applicable policies, procedures, laws, and regulations, including 8 C.F.R. § 208.6, "Disclosure to Third Parties". In particular, FDNS Immigration Officers receive training on how to evaluate Pangaea Text findings, how to record relevant findings

[29] *See* https://marketplace.fedramp.gov/#/product/aws-us-eastwest?status=Compliant&sort=productName.
[30] Public clouds are owned and operated by third-party service providers whereas private clouds are those that are built exclusively for an individual enterprise.
[31] *See* DHS 4300A SENSITIVE SYSTEMS HANDBOOK, *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

in standardized FDNS documents, and how to use relevant findings in the course of any administrative investigations. Asylum Officers receive training on how to evaluate Pangaea Text findings, and how to use relevant findings in an asylum interview and adjudication.

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

USCIS uses role-based access controls and enforces a separation of duties to limit access to only those individuals who have a need-to-know in order to perform their duties. Each operational role is mapped to the set of system authorizations required to support the intended duties of the role. The mapping of roles to associated authorizations enhances adherence to the principle of least privilege. Authorized users are broken into specific classes with specific access rights. This need-to-know is determined by the respective responsibilities of the employee. These are enforced through DHS and USCIS access request forms and procedures. In Pangaea Text, there are distinct user roles for Asylum Officers and FDNS Immigration Officers based on their respective responsibilities.

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 request for the system must go through the USCIS Change Control Process and must be approved by the proper authorities of this process, such as the USCIS Privacy Officer, Chief of Information Security Officer, Office of Chief Counsel, and the respective Program Office.

Responsible Official

Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
U.S. Department of Homeland Security
(202) 272-8030

Approval Signature

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

Appendix A –
Information Collected on Form I-589

Information collected on the I-589[32] includes:

- Alien registration number;
- Social Security number (SSN);
- USCIS online account number;
- First name;
- Middle name;
- Last name;
- Aliases;
- Current address and phone number;
- Mailing address and phone number;
- Gender;
- Marital status;
- Date of birth;
- City and country of birth;
- Present nationality;
- Nationality at birth;
- Race, ethnic, or tribal group;
- Religion;
- Immigration court history;
- Date applicant last left their country;
- Current I-94 number;
- History of travel to the U.S. (including date, place of entry, status, and date status expires);

[32] Pursuant to Executive Order 13780, *Protecting the Nation From Foreign Terrorist Entry*, USCIS is in the process of modifying Form I-589 to include high value and social media data fields.

- Passport information (including country of issuance, passport or travel document number, and expiration date);
- Languages spoken;
- Information about spouse and children;
- Residential, educational, and work history;
- Information about parents and siblings;
- Information about harmed suffered by the applicant or family or friends/colleagues;
- Information about feared harm;
- Information about arrest and criminal history for the applicant and their family;
- Involvement by the applicant or their family in any groups or organizations;
- Information about whether or not the applicant or their family have applied for refugee status, asylum, or withholding of removal before;
- Travel pattern of the applicant and their family on the way to the United States;
- Return trips to home country, and whether or not they applied for or received lawful status in another country;
- Participation in harming any other individual, if any;
- Whether applicant filed more than one year after coming to the United States, and if so, why; and
- Information about preparation of the application.