Privacy Impact Assessment
for the

Fraud Detection and National Security Directorate

DHS/USCIS/PIA-013-01

December 16, 2014

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

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
202-343-1717

Abstract

The Department of Homeland Security, United States Citizenship and Immigration Services created the Fraud Detection and National Security (FDNS) Directorate to strengthen the integrity of the nation's immigration system and to ensure that immigration benefits are not granted to individuals that may pose a threat to national security and/or public safety. In addition, the FDNS Directorate is responsible for detecting, deterring, and combating immigration benefit fraud. The United States Citizenship and Immigration Services conducted this Privacy Impact Assessment (PIA) to document and assess how the Fraud Detection and National Security Directorate collects, uses, and maintains personally identifiable information. USCIS is updating and reissuing this PIA, originally published on July 30, 2012 as DHS/USCIS/PIA-013(a), to include FDNS's sharing with Law Enforcement Agencies and include the DHS/USCIS/ICE/CBP-001-Alien File, Index and National File Tracking System of Records, published November 21, 3013 at 78 FR 69864 as coverage for initiatives under this PIA.

Overview

The Department of Homeland Security (DHS) United States Citizenship and Immigration Services (USCIS) implements immigration law and policy through the processing and adjudication of applications and petitions submitted for citizenship, asylum, and other immigration benefits. Benefits may include adjustment of immigration status (granting lawful permanent residence), naturalization (granting United States citizenship), asylum and refugee status, and other immigrant and nonimmigrant benefits. USCIS supports the DHS statutory mandate of protecting the nation by identifying applicants who threaten national security or public safety and denying them immigration benefits that would allow them to legally enter or remain in the United States. In addition, USCIS enhances the integrity of the nation's legal immigration system by detecting and deterring immigration benefit fraud. In order to support this DHS statutory mandate, USCIS collects applicant, petitioner, and beneficiary information to adjudicate applications and petitions so that immigration benefits are only granted to eligible individuals in an accurate, efficient, and timely manner.[1] This information is also used to determine if and when those benefits should be rescinded or revoked.

In 2004, USCIS established the Fraud Detection and National Security Directorate (FDNS) in response to a Congressional recommendation to establish an organization "responsible for developing, implementing, directing, and overseeing the joint USCIS-Immigration and Customs Enforcement (ICE) anti-fraud initiative and conducting law enforcement/background checks on every applicant, beneficiary, and petitioner prior to granting immigration benefits."[2] FDNS fulfills the USCIS mission of enhancing both national security and the integrity of the legal immigration system by: (1) identifying threats to national security and public safety posed by those seeking immigration benefits; (2) detecting, pursuing,

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

[2] Conference Report to accompany H.R. 4567 [Report 108-774], "Making Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 30, 2005," p. 74, *available at* http://www.gpo.gov/fdsys/pkg/CRPT-108hrpt774/pdf/CRPT-108hrpt774.pdf.

and deterring immigration benefit fraud; (3) identifying and removing systemic vulnerabilities in the process of the legal immigration system; and (4) acting as USCIS's primary conduit for information sharing and collaboration with other governmental agencies. FDNS also oversees a strategy to promote a balanced operation that distinguishes USCIS's administrative authority, responsibility, and jurisdiction from ICE's criminal investigative authority.

FDNS serves as the primary liaison between USCIS and the law enforcement and intelligence community. This effort includes establishing and developing relationships and collaborating with law enforcement; intelligence; and federal, state, and local agencies to ensure criminals, terrorists, and other individuals who pose a threat to national security and/or public safety are not able to exploit the immigration system to gain access to, or remain in, the United States. In addition, FDNS works with adjudications on cases of suspected fraud and where the security vetting process has indicated possible national security or public safety-related concerns (please see the Appendix for a detailed description of the FDNS vetting initiatives).

There are two main personnel positions in USCIS discussed in this document —the FDNS Immigration Officer (FDNS IO) and the Adjudications Immigration Services Officer (ISO). FDNS IOs perform administrative investigations to obtain relevant information needed to render the appropriate adjudicative decision. Upon conclusion of an administrative investigation, FDNS IOs report their findings to USCIS adjudications. The ISO makes the adjudicative decision. These two entities — FDNS IOs and Adjudications ISOs — work together to ensure that fraud, national security, and public safety concerns are fully investigated prior to the decision on a benefit.

Headquarters Operations

Headquarters FDNS (HQFDNS) develops, oversees, and maintains policies, procedures, and other efforts within USCIS's administrative authorities to detect, identify, and combat threats to the security of the United States and the integrity of its legal immigration system. This includes collaboration with law enforcement; intelligence; and federal, state, and local agencies to ensure criminals, terrorists, and other individuals posing a threat to public safety or national security are not able to exploit the legal immigration system to gain access to, or remain in, the United States. USCIS and ICE, which is responsible for the criminal investigation and prosecution of immigration benefit fraud, have implemented a joint anti-fraud strategy through FDNS. This strategy promotes balanced operations that distinguish USCIS' administrative authority, responsibility, and jurisdiction from ICE's criminal investigative authority.

HQFDNS also works with other components of USCIS to develop operational policy to detect fraud, and to identify and combat threats to security. Field Operations (FOD); Service Center Operations (SCOPS); and Refugee, Asylum, and International Operations (RAIO) directorates supervise field FDNS Immigration Officers. HQFDNS develops and implements operational policies and procedures that address fraud and national security concerns in coordination with these directorates. FDNS also works with the Enterprise Services Directorate (ESD) on policies and procedures related to biometric and other security checks. In addition, the USCIS Privacy and Office of the Chief Counsel advise FDNS on the privacy and legal considerations of policies and initiatives.

HQFDNS consists of three operational divisions: the National Security Division, the Fraud Division, and the Intelligence Division, all of which provide guidance to field and HQ FDNS IOs. HQFDNS does not directly supervise FDNS IOs in the field, but provides operational policy and guidance to FDNS field IOs.

National Security Division

The National Security Division (NSD) is responsible for developing agency policies, procedures, priorities, and objectives relating to the detection and resolution of national security concerns in immigration benefit petitions and applications. NSD focuses on: (1) the national security vetting processes; (2) oversight of procedures for handling national security concerns; and (3) information sharing with the law enforcement and intelligence community. NSD works closely with the Intelligence Division (ID) to ensure coordination within USCIS.

Improving National Security Vetting

NSD develops and monitors the protocol that FDNS IOs must follow when a potential national security concern has been identified during the vetting of individuals who have requested an immigration benefit. NSD provides technical assistance to FDNS IOs and ISOs in the field when vetting has identified a possible national security concern. This includes reaching out to partner agencies to resolve any such concerns and providing information for use in the adjudication process. The NSD Screening Coordination Office (SCO) reviews the existing processes for national security vetting, which includes national security and criminal checks and identifying areas for improvement.

Conducting Oversight

NSD is responsible for tracking and reporting the volume of national security workload within USCIS. NSD regularly reports processing information to leadership to ensure these special cases are receiving proper attention.

Facilitating Information Sharing

In addition to its security vetting responsibilities, NSD serves as the primary oversight entity for HQFDNS employees detailed to other government agencies to facilitate information sharing with the law enforcement and intelligence community. These officers have access to USCIS information and facilitate efficient and appropriate information sharing. In addition, they serve as subject matter experts regarding immigration laws and policies. NSD also handles the adjudication of sensitive cases sponsored by other government agencies.

Fraud Division

The Fraud Division (FD) is responsible for developing and overseeing anti-fraud policies and procedures, detecting fraudulent immigration activities, and identifying fraudulent benefit applications. FD is also responsible for developing operational policy and administering the Administrative Site Visit and Verification Program (ASVVP), a program in which FDNS IOs and contractors conduct random, administrative site visits to the work sites of petitioners and beneficiaries of religious workers and certain employment-based benefits.

Intelligence Division

The Intelligence Division (ID) is responsible for representing USCIS interests to the DHS Office of Intelligence and Analysis (I&A), the DHS Operations Coordination and Planning, and other agencies within the law enforcement and intelligence community. ID manages the analysis, reporting, production, and dissemination of USCIS immigration-based intelligence products both in the field and at HQFDNS. These products provide information on patterns, trends, and indicators of fraud or national security concerns. ID is also responsible for preparing specific intelligence reports addressing national security and/or public safety concerns involving immigrants and/or immigration processes, as well as for responding to internal and external requests for information (RFI) through the DHS I&A single point of service.

FDNS Operations in the Field

FDNS IOs are located at all USCIS service centers, field offices, asylum offices, and some overseas offices and are directly supervised by their respective field leadership. FDNS IOs are responsible for conducting administrative inquiries into suspected benefit fraud and aiding in the resolution of national security or criminal concerns. FDNS IOs may also refer egregious public safety cases, national security concerns, and fraud cases to ICE.

To initiate the administrative inquiry process,[3] FDNS IOs receive written fraud, national security, and criminal referrals from ISOs. FDNS IOs may also receive referrals or Requests for Assistance (RFA)[4] from law enforcement partners and internal USCIS entities, or tip letters from the public. FDNS IOs perform systems checks and research on the subject of the referral and then determine whether to take any further action or decline the referral. If an investigation is deemed necessary, FDNS IOs will perform further checks in USCIS, DHS, and federal databases, as well as public information[5] to verify information provided on, and in support of, applications and petitions. If a referral is declined, FDNS IOs record the case in the FDNS Data System (FDNS-DS), which is described below, and return the case to the ISO with the reason for declination.

In conducting an administrative inquiry, FDNS IOs may perform one, or a combination, of the following:

- research in government and commercial databases and public records;
- Internet searches of open source information;
- searches of social media sites;
- file reviews;

[3] USCIS conducts administrative inquiries, ICE conducts criminal investigations.
[4] RFAs may be satisfied with subject matter expertise, operational assistance, information, or a combination of any of these. RFAs may be made by USCIS officers, in addition to external law enforcement and intelligence organizations.
[5] Public information includes any open source information legally accessible by anyone such as records of tax liens, court documents, and information drawn from the Internet.

- telephone calls;
- site visits;
- interviews of applicants, beneficiaries, petitioners, and others;
- requests for evidence;
- administrative subpoenas;
- requests for assistance; and
- overseas verifications.

In addition to FDNS-DS, FDNS uses an unclassified SharePoint Services-based repository to manage internal policy and operational documents, content, and reports. Role-based access is granted for officers with a need to know. The repository provides a secure environment to facilitate collaboration among HQFDNS personnel and between HQFDNS and its field officers. The data are protected using security safeguards established by DHS.

In keeping with the audit controls and role-based access safeguards established under the DHS SharePoint and Collaboration Sites PIA,[6] the FDNS SharePoint site has a designated site owner, or administrator, responsible for determining the user base and ensuring the site is only used for approved purposes such as internal collaboration and document and workflow management. The site owner ensures that only users with a verifiable need to know have access privileges to the information on the FDNS SharePoint site. The FDNS SharePoint environment includes a template with a "Sensitive Personally Identifiable Information Allowed" banner at the top of pages approved to manage and share sensitive PII. In addition, the FDNS SharePoint site follows the compliance restrictions placed on SharePoint usage by completing this PIA and the accompanying SORNs. FDNS regularly reviews the information posted to the SharePoint site, and if inappropriate posting of PII is discovered, FDNS ensures its immediate removal from the site and reports the posting as a privacy incident.

Social Media Sites

USCIS is finalizing its policy for use of Social Media in compliance with the DHS Directive 110-01, Privacy Policy for Operational Use of Social Media and Instruction 110-01-001. When completed, FDNS IOs will be permitted to access social media sites when conducting administrative investigations only after they have completed an annual training on use of social media and signed a "Rules of Behavior" form. When conducting official government business, FDNS IOs will not establish accounts on social media sites using fictitious names or information, or use personal accounts for official government business. FDNS IOs must use government-issued equipment to access social media. FDNS IOs cannot communicate with users of social media sites, and may only passively review information. Further, any information, whether it is derogatory or not, found on a social media site that is used in an investigation must be printed and saved in the applicant's file and electronically within FDNS-DS. As with all derogatory information found from publicly available sources, the applicant and/or petitioner

[6] See DHS/ALL/PIA-037 DHS SharePoint and Collaboration Sites, *available at* www.dhs.gov/privacy.

must be provided with an appropriate opportunity to explain or refute any information that conflicts with information he or she provided to USCIS before a decision is made regarding the requested benefit.[7]

Access to these sites is helpful to FDNS in that the information contained therein may facilitate validation or invalidation of information provided by the applicant and/or petitioner. Although USCIS does not deny benefits solely based on publicly available information, the FDNS IO provide information found in open sources for USCIS adjudications personnel to formulate a Request for Evidence (RFE), a Notice of Intent to Deny (NOID) to the applicant or petitioner, or during an interview with the petitioner and/or beneficiary. The applicant and/or petitioner will have the opportunity to explain and resolve any inconsistencies among information sources prior to issuance of an adjudicative decision. The applicant and/or petitioner will have an opportunity to file motions or appeals if the application or petition is denied.

Administrative Site Visit and Verification Program (ASVVP)

HQ FDNS developed the Administrative Site Visit and Verification Program (ASVVP). Under ASVVP, field FDNS IOs and contractors conduct site inspections to verify information, better identify and target fraud cases for follow-up, and when appropriate, refer cases to ICE for investigation. Currently, all religious organizations are subject to site inspections/compliance reviews prior to adjudication of Form I-360 (Petition for Amerasian, Widow(er), or Special Immigrant) or Form I-129 (R) (Petition for a Nonimmigrant Worker). In addition, site inspections are conducted on H-1B applications (foreign workers in specialty occupations) after adjudication of extension or change of status requests. Field FDNS IOs and contract site inspectors verify information submitted with the petition, including supporting documentation submitted by the petitioner. Field FDNS IOs and contract site inspectors also verify the existence of the petitioning entity, take digital photos, review documents, and speak with organizational representatives to confirm the beneficiary's work location, employment workspace, hours, salary, duties, and overall employer-employee relationship. Field FDNS IOs record their findings in FDNS-DS and submit a report to the case adjudicator for final determination. Contract site inspectors submit their findings to Field FDNS IOs, who consider the information in determining whether the petitioner and beneficiary are in compliance with the terms and conditions outlined in the petition and the Field FDNS IOs forward a report on to the case adjudicator for final determination. Petitioners are given the opportunity to address USCIS's derogatory findings.

Fraud Detection and National Security Data System

The Fraud Detection and National Security Data System (FDNS-DS)[8] is a central data repository that FDNS IOs use to record, track, and manage the background check process related to immigration applications and petitions, as well as information related to beneficiary applications with suspected or confirmed fraud, criminal activity, public safety and/or national security concerns, and cases randomly selected for benefit fraud assessments. FDNS-DS maintains information on all individuals who have been reviewed for these concerns. In instances where no fraud, criminal activity, public safety and/or national security concerns were found, the information maintained may be used to demonstrate an

[7] 8 CFR § 103.2(b)(16).
[8] *See* DHS/USCIS/PIA-013 FDNS-DS PIA, *available at* www.dhs.gov/privacy.

assessment was conducted so that additional resources do not have be used for a second review.

FDNS IOs may share FDNS-DS data with law enforcement and intelligence agencies in response to Requests for Information (RFIs) to support criminal and administrative investigations and background checks involving immigrant benefit fraud, criminal activity, and public safety and/or national security concerns. For example, information may be shared with the Department of State (DOS), Bureau of Consular Affairs to provide a comprehensive picture of a visa applicant's status, and to reduce the likelihood that an individual or group might fraudulently obtain an immigration benefit under the INA, as amended. Also, selected ICE representatives have "read-only" access to FDNS-DS, which allows them access and use of the most current information for purposes of criminal investigations.

Furthermore, this PIA is now covered by both DHS/USCIS-006 FDNS Records System of Records Notice (SORN) and DHS/USCIS/ICE/CBP-001 Alien File [A-File], Index and National File Tracking (A-File SORN).[9]

This PIA replaces the FDNS Directorate PIA published on July 30, 2012.

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 INA, 8 U.S.C. § 1101, *et seq.* provides the legal authority to collect information used for the adjudication of immigration benefits. In addition to other delegations, the Secretary of Homeland Security in Homeland Security Delegation No. 0150.1 paragraphs (H), (I), (J), (M), and (S) has delegated the following authorities to USCIS:

- Authority under section 103(a)(1) of the INA, as amended, 8 U.S.C. § 1103(a)(1), to administer the immigration laws (as defined in Section 101(a)(17) of the INA);
- Authority to investigate alleged civil and criminal violations of the immigration laws, including but not limited to alleged fraud with respect to applications or determinations within the Bureau of Citizenship and Immigration Services (BCIS) [predecessor to USCIS] and make recommendations for prosecutions or other appropriate action when deemed advisable;
- Authority to fingerprint and register aliens;
- Authority to maintain files and records systems as necessary; and
- Authority to take and consider evidence.[10]

The joint USCIS-ICE anti-fraud strategy was established by the *Conference Report, FY 2005*

[9] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (November 21, 2013); DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (August 8, 2012).

[10] *See* DHS Delegation No. 0150.1 (effective March 1, 2003).

Appropriations Act.[11] The Appropriations Act authorized USCIS to conduct law enforcement and background checks on every applicant, beneficiary, and petitioner prior to granting immigration benefits.

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

The following SORNs cover the information that is collected, used, disseminated during the course of FDNS functions:

- DHS/USCIS-006 - FDNS SORN[12]
- DHS/USCIS/ICE/CBP-001 - A-File SORN[13]

These SORNs cover the records maintained in the Fraud Detection and National Security Data System (FDNS-DS) as well as records maintained in other collaborative workspaces specifically set up for FDNS and any paper records. Furthermore, the A-File SORN covers the use of the A-File for the purpose of detecting, deterring, and combating immigration benefit fraud.

Finally, FDNS information derived from other USCIS systems is covered under that system's respective SORN until there is an indication of possible fraud, public safety or national security concern, or criminal concern referred to FDNS by the public, other agencies, or USCIS employees.

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

Yes. The USCIS Office of Information Technology has completed and implemented a system security plan, which complies with the Federal Information Security Management Act (FISMA). FDNS-DS has also completed the Certification and Accreditation process and received an Authority to Operate, granted in August 2011, which is effective through 2014.

The FDNS SharePoint sites are protected using security safeguards established by DHS.[14] The privacy risks associated with the use of SharePoint to manage assets containing PII and/or SPII are misuse of information, data spills, and unauthorized account access. To mitigate these risks, the FDNS SharePoint site has a designated site owner, or administrator, responsible for determining the user base and ensuring the site is only used for approved purposes such as internal collaboration and document and workflow management. The site owner ensures that only users with a verifiable need to know have access privileges to the information on the FDNS SharePoint site. In addition, the FDNS SharePoint site follows the compliance restrictions placed on SharePoint usage through this PIA and the FDNS Records

[11] Conference Report to accompany H.R. 4567 [Report 108-774], "Making Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 30, 2005," p. 74, *available at* http://www.gpo.gov/fdsys/pkg/CRPT-108hrpt774/pdf/CRPT-108hrpt774.pdf.

[12] DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (August 8, 2012).

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

[14] *See* DHS/ALL/PIA-037 DHS SharePoint and Collaboration Sites, *available at* www.dhs.gov/privacy.

and A-File SORNs.[15]

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

Yes. The Retention Schedule for FDNS [N1-566-08-18] was approved on June 25, 2008. NARA approved a records retention schedule of 15 years from the date of the last interaction between FDNS personnel and the individual for records maintained in FDNS and its associated subsystems. Records related to an individual's A-File are transferred to his or her A-File and maintained under the A-File retention period [N1-566-08-11]. USCIS retains A-File records for 100 years from the individual's date of birth, and then transfers the records to NARA.

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.

There are no forms associated with this collection. However, FDNS may collect data from USCIS applications and petitions that are covered by the PRA. See the CLAIMS 3 and CLAIMS 4 PIAs[16] for more information on the various forms that cover the initial collection of information from the individual.

Section 2.0 Characterization of the Information

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

When FDNS initiates or considers a case for administrative inquiry because of suspected or confirmed fraud, criminal activity, public safety and/or national security concerns, or reviews a case randomly selected for benefit fraud assessments, it will collect and use some or all of the following data:

- Individual's name;
- Alias(es);
- Social Security number (SSN);
- Alien Number (A-Number);
- Associated A-Numbers of close relatives and associates;

[15] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (November 21, 2013); DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (August 8, 2012).

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

- Application Receipt Number;
- Address (home and business);
- Date of birth;
- Place of birth;
- Driver's License number;
- Country of citizenship;
- Citizenship status;
- Gender;
- Telephone number(s);
- E-mail address;
- Place of employment and employment history;
- Associated organizations (e.g., corporate information relating to employing entity if employment-based immigration benefits are being sought, and place of business or place of worship if such organization is sponsoring the applicant);
- Family lineage;
- Bank account information and/or financial transaction history;
- Marriage record;
- Civil or criminal history information;
- Publically available information provided by the applicant on social media websites;
- Education record;
- Information from commercial data providers in order to verify information provided on the application;
- Biometric identifiers (e.g., photographic facial image, fingerprints, signature);
- TECS, National Crime Information Center, and data and analysis resulting from the investigation or routine background checks performed as part of the adjudication process; and
- Other unique identifying numbers or characteristics such as passport number(s), visa number(s), account numbers, and identifiers associated with travel.
- FDNS-DS will also maintain the status of a particular case whether it is open or closed, what information was passed to the ISOs, and the recommendation made to ISO.

FDNS may also retain information on Representatives and Preparers in the event their information is linked to a case in FDNS-DS. Collected information includes the following data:

- Representative and/or Preparer information maintained in the Form G-28, *Notice of Entry of Appearance as Attorney or Accredited Representative*;
- Name;
- Address;
- Phone number;
- Fax number;
- Email address;
- Bar number;
- State of bar membership;
- Date of filing; and
- Associated client case information.

In addition, FDNS may gather additional data on Representatives or Preparers that are the subject or associated with a fraud, public safety, or national security concern based on applications submitted on behalf of individuals seeking an immigration benefit.

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

FDNS collects and maintains information on individuals with suspected or confirmed fraud, criminal activity, public safety and/or national security concerns, and cases randomly selected for benefit fraud assessments. In order to carry out this mission, FDNS collects information from multiple sources and stores it in FDNS-DS. In addition to FDNS-DS, FDNS uses an unclassified Sharepoint Services-based repository to manage internal policy and operational documents, content, and other information relating to cases. The repository provides an environment to facilitate collaboration among HQFDNS personnel and between HQFDNS and its field offices. This data is protected using security safeguards established by DHS.

The sources include applications and supporting documents submitted by the applicant; interviews with current/past employers, family members, petitioners or applicants; results of ASVVP site visits; direct access to other federal law enforcement systems; information obtained from commercial data providers; state and local government databases; and public source information, such as newspapers and/or the internet. Information is also compiled during the process of answering RFIs from law enforcement and intelligence agencies, as well as when FDNS refers cases to law enforcement entities such as ICE and the Federal Bureau of Investigation (FBI).

USCIS Sources

- USCIS Electronic Immigration System (USCIS ELIS)
- Service Center Computer Linked Adjudication Information Management System (SCCLAIMS);
- Benefits Biometric Support System (BBSS);
- Enterprise Service Bus/Person Centric Query System (ESB/PCQS);
- CLAIMS 3;
- CLAIMS 4;
- Central Index System (CIS);
- Change of Address Form (AR11 System and Form);
- Refugee, Asylum, and Parole System (RAPS);
- Asylum Pre-Screening System (APSS);
- Interim Case Management Solution (ICMS);
- Customer Profile Management System (CPMS);
- National File Tracking System (NFTS);
- Enterprise Citizenship and Immigration Service Centralized Oracle Repository (eCISCOR);
- External Data Interface Standards (EDIS);
- Customer Representative System;
- Validation Initiative for Business Enterprise (VIBE);
- Scheduling Notification for Applicant Processing (SNAP); and
- Electronic Document Management System (EDMS).

Other DHS Sources

- U.S. Customs and Border Protection (CBP) TECS;
- CBP Arrival and Departure System (ADIS).

- DHS National Protection and Programs Directorate (NPPD) Automated Biometric Identification System (IDENT); and

Other Federal Agency Sources

FDNS receives information from the FBI on applicants as a result of fingerprint and name checks. FDNS may also receive information from the DOS's Consular Consolidated Database (CCD) and other government databases when needed to address national security concerns and facilitate pilot programs.[17]

As part of the RFI where USCIS is requested to provide relevant information to another agency for law enforcement, national security, and/or fraud purposes, the request will be maintained in FDNS-DS along with any response.

For an RFA process where USCIS is requesting information on a particular individual or group of individuals, FDNS maintains the information requested and provided from other agencies in FDNS-DS. This information is compiled during the process of reviewing and answering requests for assistance or information from law enforcement and intelligence agencies, as well as when FDNS refers cases to law enforcement components such as ICE and the FBI.

Public Sources, including Commercial Data

FDNS uses a number of open source and publicly available web-based resources when investigating potential fraud leads or cases with national security and intelligence implications. The use of public and commercial sources is discussed in detail below.

Other Data Sources

Finally, FDNS receives information from external governmental and non-governmental entities related to suspected fraud, public safety, and national security concerns. FDNS may receive unsolicited information regarding applications and petitions by outside parties via email, letter, phone call, or in-person. Any information received through these methods may be considered in the adjudication process, but will not be relied upon as the sole basis for an adverse determination by USCIS. Rather, the applicant and/or petitioner will have the opportunity to provide additional information to explain and resolve any discrepancies produced as a result of this information. This information may contain PII and is handled in accordance with DHS and USCIS policy and procedures, including this PIA and accompanying SORNs.

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

Yes. FDNS obtains information from a limited number of commercial data providers and manually records relevant data in FDNS-DS. FDNS also consults public sources such as the Internet, social media, news feeds, and state and local public records, including court records, to verify the historical, biographical, financial, and personal information presented by applicants to detect the possibility of immigration benefit fraud and public safety and national security concerns.

In addition to FDNS-DS, FDNS uses an unclassified Sharepoint Services-based repository to manage internal policy and operational documents, content, and reports. The repository provides an environment to facilitate collaboration among HQFDNS personnel and between HQFDNS and its field officers. If during the search of publicly-available sources FDNS identifies relevant information to a case, it will maintain it in either FDNS-DS or the FDNS SharePoint Services site pursuant to the FDNS

[17] *See* Appendix A.

SORN.[18] FDNS does not make fraud, national security, and/or public safety determinations solely on this publicly-available information; rather, FDNS uses it as a verification of information already provided by the applicant and/or petitioner. The applicant and/or petitioner will be provided the opportunity to refute any inconsistencies arising from commercial, public records, or publicly available data sources.

2.4 Discuss how accuracy of the data is ensured.

All information obtained by FDNS IOs and reviewed by ISOs is reviewed in accordance with a strict set of internal procedures intended to ensure that actionable derogatory information meets the standards for evidence established by the USCIS Administrative Appeals Office, the Department of Justice (DOJ), Executive Office for Immigration Review (EOIR), and the federal court system. Most of the information collected and maintained within USCIS systems is provided directly from immigration benefit applicants. FDNS-DS primarily relies on information collected by other USCIS systems at the point of application intake and therefore relies on the accuracy of those systems. In addition, all USCIS forms notify the applicant and petitioner that information provided may be further verified and, in many cases, in-person interviews are conducted to ensure the accuracy of the provided information.

FDNS incorporates strenuous verification procedures to ensure accuracy of data before an immigration benefit decision is made by adjudications. These procedures include direct queries of DHS and other government agency databases as well as USCIS ISO interviews with applicants or petitioners. Public source information is used to verify or identify inconsistencies with information provided by applicants or petitioners as part of their application for immigration-related benefits. In any case where USCIS contemplates denial, rescission, or revocation of an immigration benefit based on evidence of fraud, the petitioner or applicant will be given an opportunity to review and rebut the evidence.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of collecting more information than necessary.

Mitigation: FDNS collects extensive information on individuals in the course of a review of possible national security concerns, public safety threats, or indications of fraud. FDNS has determined that in order to have the best evidence available to support a case, it is necessary to collect large amounts of sensitive PII. This information is required to ensure that FDNS makes the correct determination about the correct individual regarding national security, public safety, or fraud cases and enables adjudications to make a decision on the benefit application.

Privacy Risk: There is a risk in relying on data obtained through commercial data, public sources, or social media since that information may be inaccurate.

Mitigation: Public source information is not used as the sole basis upon which to deny an immigration benefit, investigate benefit fraud, or identify public safety and national security concerns due to the inherent lack of data integrity. The commercial source and public information is used to attempt to identify immigration benefit fraud and public safety and national security concerns by comparing

[18] *See* DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (August 8, 2012).

historical, biographical, financial, and personal information presented by the immigration benefits applicant or petitioner against third-party sources, wherever possible.

All FDNS Officers are trained to consider information derived from sources other than the applicant and/or petitioner, but are also cautioned about its accuracy. Due to its inherent lack of data integrity, public source information is not used as the sole basis upon which to deny an immigration benefit, investigate benefit fraud, or identify public safety and national security concerns.

Privacy Risk: There is a risk of obtaining data from new sources that have not been approved for use in determining possible benefit fraud, public safety, and national security concerns.

Mitigation: In order to reduce the risk of new data being incorporated into FDNS that has not been reviewed for privacy and legal concerns, this PIA has been drafted to allow routine review of new data sources and updates to be made as necessary. Additionally, DHS has issued a directive on the use of social media web sites to bring additional education to the risks of using such data sources.

Privacy Risk: There is a risk of obtaining inaccurate data.

Mitigation: In order to improve the accuracy of the information, USCIS has developed policies and procedures for safeguarding data aggregated within FDNS from several different sources. This includes using public record data, data from commercial data providers, as well as other publicly available data including social media and news and reviewing existing data in USCIS's files with information outside of USCIS. If inaccurate information is found during the process of reviewing a file, FDNS will contact personnel within the USCIS Records Division who are authorized to make the changes to the data in the source system. FDNS will also correct inaccuracies in FDNS-DS and other locations where FDNS records are maintained. Additionally, if information is found that will impact whether an individual is granted a benefit, the individual will be provided the opportunity to review the information.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

FDNS-DS is the central data repository that permits HQ and Field FDNS IOs to record, track, and manage the background check and adjudicative process related to immigration applications and petitions, as well as beneficiary applications with suspected or confirmed fraud, criminal activity, public safety and/or national security concerns, and cases randomly selected for benefit fraud assessments. In addition to FDNS-DS, FDNS has created collaborative workspace that allows employees in HQ and the field share information consistent with the SORNs for FDNS records.[19]

The information collected and maintained within FDNS system of records is used as part of a variety of National Security Vetting Initiatives to determine benefit fraud, criminal activity, public safety, and national security concerns within the immigration benefit determination process. FDNS-DS is used as a central repository of information collected from the applicant, other government databases, and open

[19] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (November 21, 2013); DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (August 8, 2012).

sources to assist HQ and FDNS IOs in determining whether immigration fraud or other criminal acts have occurred. FDNS also uses the information to determine whether there may be additional cases that might be associated with identified fraud schemes or national security concerns. FDNS conducts different pilots to identify improvements in its security vetting. FDNS will use the PTA process and the appendix to this PIA to document the new processes, including sharing agreements.

Commercial data, public records, data from social media web sites and publicly available data are also used to help validate or identify inconsistencies with information already on file as part of an application with USCIS; however, the information is not used as the sole basis upon which to deny an immigration benefit.

Any additional data may be stored in FDNS-DS or in an appropriate location in the FDNS SharePoint Services site. Case information is stored and managed in FDNS-DS. SharePoint allows officers to access informational reports that may contain individual case information.

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. Neither FDNS-DS nor the other information technology tool run pattern-based queries or searches for FDNS. FDNS-DS only runs reports to allow employees to analyze data relating to cases involving suspected fraud, public safety, or national security. FDNS may use the results to facilitate the identification of fraud patterns or trends, as well as previously unknown associations between applicants involved in fraud who pose national security or public safety concerns. FDNS will place the information it collects, derogatory or not, in the FDNS-DS record for each individual.

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

A limited number of ICE personnel have “read-only” access to FDNS-DS. FDNS may share specific information with ICE to determine whether criminal investigation or law enforcement action is required. In addition, FDNS may share information with DHS I&A if a potential nexus to terrorism is identified or if the information has intelligence value. Only FDNS employees have access to the collaborative workspace.

When another DHS component such as CBP requests information on an individual because of concerns related to fraud, criminal activity, public safety and/or national security, FDNS IOs review the request, log it in FDNS-DS, and provide the requested information to the component, as appropriate. Responsive information will be shared via secure government networks. FDNS information may be used to assist CBP in their decision on whether to allow an alien to enter the country.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information contained within FDNS system will not be used consistent with its original purpose and authority.

Mitigation: Consistent with FDNS's mission of detecting, deterring, and combating immigration benefit fraud, all information contained within FDNS is used to identify and track possible benefit fraud, criminal activity related to immigrants and non-immigrants, public safety, and national security concerns. These uses are consistent with the notice provided to individuals in the Privacy Act Statements on all USCIS forms, as well as this PIA and the corresponding SORNs.[20]

Privacy Risk: There is a risk that use of commercial or publicly available information, including social media, may contribute to an erroneous adverse effect on an individual, such as denial of an immigration benefit.

Mitigation: Information collected from commercial and public data sources are only used to corroborate and enhance information obtained by USCIS directly from an individual during the immigrant benefit application process. Immigration benefit determinations are not based solely on commercial and public data, but instead this information is used to corroborate an individual's identity or benefit claim requests. FDNS trains IOs on the appropriate use of commercial and public source information to preserve the data accuracy and integrity of the original information submitted by the applicant.

There is also a risk that new information produced during the research and investigation process may be inaccurate or incorrect and may lead to the determination of a denial of a benefit for an individual. Public source information is only used to verify or identify inconsistencies with information provided by applicants or petitioners as part of their application for immigration-related benefits. In any case where USCIS contemplates denial, rescission, or revocation of an immigration benefit based on evidence of fraud, the petitioner or applicant will be given an opportunity to review and rebut the evidence.

Additionally, USCIS maintains audit logs for all individuals who access social media websites, and these, along with information placed into FDNS-DS as the result of social media use, are reviewed periodically by the USCIS Privacy Officer for compliance with DHS policy on use of social media websites.

Privacy Risk: There is a risk of an inappropriate assumption that all individuals listed within FDNS-DS or other FDNS records maintained outside of FDNS-DS have engaged in fraudulent immigration-related practices or pose a public safety or national security risk.

Mitigation: Cases within FDNS-DS as well as the collaborative workspace that are resolved without a finding of fraud are documented clearly in FDNS-DS. These cases are marked with "no fraud found" and contain a statement of findings within the system. This statement will contain a summary of the case and FDNS IO's recommendations to ISOs as to fraud and/or national security concerns.

Privacy Risk: For certain security vetting projects, FDNS must make a copy of the data in FDNS-DS and share with other IT systems. There is a risk that data will be inaccurately copied. There is

[20] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (November 21, 2013); DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (August 8, 2012).

also a risk that the data may be taken out of context.

Mitigation: FDNS reconciles data to ensure that the data transferred from FDNS-DS to other systems is transferred accurately and completely. FDNS performs regular audits if an ongoing feed is used. FDNS also ensures that the data copied out of FDNS-DS and the collaborative workspace are deleted at the end of any security vetting projects. If information from FDNS-DS is shared with individuals who are not regular users of the system, FDNS will train the user or reviewer to ensure that the nature and purpose of the data in FDNS system is understood.

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.

Notice is provided to all applicants/petitioners at the time of collection through a Privacy Act Statement on all USCIS forms. Records within FDNS are primarily based on records from underlying USCIS systems, which intake the information directly from the applicant/petitioner. Notice of collection by the underlying USCIS systems performing the original collection is described in the individual PIAs and SORNs for those systems. Notice to individuals is also provided through the publication of this PIA and the corresponding FDNS and A-File SORNs.[21]

In addition to Privacy Act Statements on all USCIS forms, USCIS forms also notify the applicant and petitioner that information provided may be verified by USCIS. FDNS IOs may verify information by conducting interviews during site visits. Upon identifying themselves and notifying the applicant or beneficiary of the reason for the site visit, the FDNS IO will request permission to speak with an applicant, petitioner, or beneficiary immediately prior to beginning the interview. Prior to scheduling an interview with an applicant or petitioner, the ISO must send a Form G-56, *Interview Notice* to the applicant and his or her attorney or accredited representative. Notice is given to an applicant's attorney when an administrative site visit or interview will occur, unless notice would jeopardize the site visit or interview.

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

Applicants who seek USCIS benefits are presented with a Privacy Act Statement and a signature-required release authorization for the relevant benefit application/petition. The Privacy Act Statement details the authority for requesting the information and purpose of the information collection. The applicant's signature on the form serves as certification that the applicant authorizes the release of any information from the applicant's record that USCIS will access to determine eligibility. Applicants are

[21] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (November 21, 2013); DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (August 8, 2012).

notified at the point of data collection (generally in the form itself) of the right to decline to provide the required information; however, such action may result in the denial of the applicant's benefit request.

The particular use policies of the underlying USCIS systems that originally collected the applicant/petitioner information from which FDNS draws and accesses data are set by those systems individually. FDNS itself does not give individuals the right to consent to particular uses of information, as doing so would limit the usefulness of the information for fraud detection and national security purposes.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals are unaware of the uses for which their information is collected.

Mitigation: Applicants for USCIS benefits are made aware that the information they are providing is being collected to determine whether they are eligible for immigration benefits through a Privacy Act Statement on the application instructions for all USCIS forms.

Section 5.0 Data Retention by the project

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

USCIS retains application information to assist in identifying applicants who threaten national security and public safety; detecting, pursuing, and deterring immigration benefit fraud; and identifying and removing systemic vulnerabilities in the process of the legal immigration system.

USCIS retains FDNS-DS records for 15 years from the date of the last interaction between FDNS personnel and the individual, no matter the determination. Upon closure of a case pertaining to an individual, any information that is pertinent to the adjudicative decision (such as a Statement of Findings (SOF)), whether there was or was not an indication of fraud, criminal activity, egregious public safety, or national security concerns, is transferred to the associated A-File. USCIS retains the A-File for 100 years from the subject's date of birth. The file is then retired to NARA for permanent storage. All data contained in other USCIS data systems, such as RAPS and CLAIMS 3, are governed by their respective retention schedules.

Records maintained in the SharePoint site follow the same retention period as FDNS-DS. SharePoint allows FDNS to note when a document is loaded onto the site, and FDNS administrators of the site will regularly review the creation date of content and remove it when the retention period expires.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that data will be retained longer than necessary. This would increase the risk of unauthorized access, use, and loss of the data.

Mitigation: FDNS mitigates this risk by destroying FDNS-DS and SharePoint data in accordance with approved NARA records retention schedules.

The 15-year retention schedule for FDNS data provides access to information that can be critical to research related to suspected or confirmed fraud, criminal activity, egregious public safety, or national security concerns for applicants/petitioners who may still be receiving immigration benefits. In addition, should the individual apply for another benefit, retention of the information can eliminate the need for research on concerns that were previously addressed. This time frame also allows FDNS to ensure that cases that were reviewed and determined to have no nexus to fraud, criminal activity, egregious public safety, or national security concerns are not opened again because old information is recycled.

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.

Yes. FDNS shares information outside of DHS when USCIS receives an RFI, when it proactively discloses based on information in the record, and when asking an outside organization for additional information related to an individual. Access may be provided through direct user accounts or through copying of data to electronic device.

Specific requests for information are governed by the originating system of records notice for the underlying USCIS records (e.g., DHS/USCIS – 007 Benefits Information System (BIS)). In such instances, USCIS may share the PII listed in Section 2.1 of this PIA with federal, state, tribal, local, international, or foreign law enforcement and intelligence agencies, in response to an RFI in support of criminal and administrative investigations and background checks involving immigrant benefit fraud, criminal activity, public safety, and national security concerns.

Through direct user account access, FDNS may share information with DOS, Bureau of Consular Affairs, to provide a comprehensive picture of a visa applicant's status and to reduce the likelihood that an individual or group might fraudulently obtain an immigration benefit under INA, as amended. DOS has read-only access to FDNS-DS.

Proactive disclosure based on information in the system occurs when FDNS has an indication of possible fraud, national security, or public safety concerns. In these cases, FDNS may proactively share information with other government entities as described under the FDNS and A-File SORNs.[22]

At the request of DHS, RFIs for national security purposes from external entities are coordinated through DHS I&A. USCIS responses are provided via government secure networks. All other requests are processed by USCIS. Responses provided by field offices are also provided via secure methods.

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

Direct account access by DOS, Bureau of Consular Affairs, is covered by FDNS SORN routine

[22] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (November 21, 2013); DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (August 8, 2012).

use I and A-File SORN routine use O, which permits USCIS to share PII with DOS, Bureau of Consular Affairs, in the processing of petitions or applications for benefits. This is compatible with the original collection under INA which requires USCIS to administer immigration laws. Information may also be shared with DOS, Bureau of Consular Affairs, to provide a comprehensive picture of a visa applicant's status, and to reduce the likelihood that an individual or group might fraudulently obtain an immigration benefit under INA, as amended.

Proactive disclosures are covered by the FDNS SORN, routine use H, which permits FDNS to share PII with federal and foreign government intelligence or counterterrorism agencies when USCIS reasonably believes there is a threat or potential threat to national or international security.

Proactive disclosures are also covered by routine use H and II of A-File SORN. Routine use H permits USCIS to share A-File information with appropriate federal, state, tribal, local, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, when DHS believes the information would assist in enforcing applicable civil or criminal laws. A-File SORN routine use II permits sharing with a federal, state, local, territorial, tribal, international, or foreign criminal, civil, or regulatory law enforcement authority when the information is necessary for collaboration, coordination, and de-confliction of investigative matters, prosecutions, and/or other law enforcement actions to avoid duplicative or disruptive efforts and to ensure the safety of law enforcement officers who may be working on related law enforcement matters.

These disclosures are compatible with the original collection because the INA requires USCIS to investigate alleged civil and criminal violations of immigration laws, including alleged fraud with respect to applications or determinations within USCIS. In addition, the INA provides for terrorist-related bars that may serve as the basis for denial of a requested benefit. The INA also requires USCIS to make recommendations for prosecutions or other appropriate actions when deemed advisable.

6.3 Does the project place limitations on re-dissemination?

Yes. A Memorandum of Agreement (MOA) between USCIS and DOS, Bureau of Consular Affairs, fully outlines responsibilities of the parties, security standards, and limits of use of the information, including re-dissemination. Methods and controls over dissemination of information are coordinated between USCIS and DOS, Bureau of Consular Affairs, prior to information sharing. Depending on the context of other sharing, DHS may place additional controls on the re-dissemination of the information.

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

FDNS maintains a record of disclosure of FDNS information made with agencies in accordance with a routine use or with whom it has an information sharing agreement. A record is kept on file of each disclosure and system audit trail logs are maintained to identify transactions performed by both internal and external users.

Field FDNS IOs are detailed to various government agencies as immigration subject matter experts. All Field FDNS IOs must abide by all privacy laws and legal requirements before sharing any immigration information.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk of misuse, unauthorized access to, or disclosure of, information.

Mitigation: As discussed above, FDNS maintains a record of each disclosure of FDNS information made with every agency in accordance with the routine use or with whom it has an information sharing agreement. A record is kept on file 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. 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 only authorized users with a need to know may have access to the information contained in FDNS-DS. DHS information is covered by the third-party discovery rule, which precludes agencies outside of DHS that have received the information from DHS from sharing with additional partners without the consent of DHS.

Risks are further mitigated by provisions set forth in MOAs or Memoranda of Understanding (MOUs) with federal and foreign government agencies and United States government employees 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?

Because FDNS contains sensitive information related to possible immigration benefit fraud and national security concerns, DHS has exempted FDNS 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. Where such a request is made, and access would not appear to interfere with or adversely affect the national or homeland security of the United States 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.

Any individual seeking to access information maintained by FDNS should direct his or her request to:

National Records Center

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

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 Access 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 CFR 5.21), and any other identifying information that may be of assistance in locating the record.

The information requested may; however, be exempt from disclosure under the Privacy Act because FDNS records, with respect to an individual, may sometimes contain law enforcement sensitive information. The release of law enforcement sensitive information could possibly compromise ongoing criminal investigations.

Additional information about Privacy Act and Freedom of Information Act (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?

The data accessed by FDNS from underlying USCIS source systems may be corrected by means of the processes described in the PIAs and SORNs for those systems. In addition, prior to using commercial, public, and other agency information to render adjudicative decisions, applicants and petitioners are given an opportunity to refute the derogatory information. Petitioners are also afforded appeal and motion opportunities. In the event inaccuracies are noted, files and FDNS-DS records will be updated.

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

Individuals are notified of the procedures for correcting their information on USCIS forms, the USCIS website, the SORNs, and this PIA.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may be unaware of their ability to make requests for access to their records in FDNS-DS.

Mitigation: Notice on how to file a Privacy Act request about records contained in FDNS-DS is provided by this PIA and the FDNS SORN. Individuals can request access to information about themselves through the Privacy Act/FOIA process, and may also request that their information be amended by contacting the National Records Center. The nature of FDNS-DS and the data it collects, processes, and stores is such that it limits the ability of individuals to access or correct their information.

Each request for access or correction is individually evaluated.

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 and security controls have been established to mitigate privacy risks associated with authorized and unauthorized uses, specifically misuse and inappropriate dissemination of data. Access to FDNS-DS is generally read-only. Some FDNS-DS users have "read," "write," and "modify" privileges. All account access and privileges are approved by the USCIS business owner. When employment at USCIS is terminated or an employee's responsibilities no longer require access to FDNS records and FDNS-DS, access privileges are removed.

Audit trails are kept in order to track and identify unauthorized uses of FDNS-DS information. The audit trails include the ability to identify specific records each user accesses. A warning banner is provided at all access points to inform users of the consequences associated with unauthorized use of information. The banner warns authorized and unauthorized users about the appropriate uses of the system, that the system may be monitored for improper use and illicit activity, and the penalties for inappropriate usage and non-compliance. A user must click on the agreement to proceed with login.

In addition, user access to FDNS-DS is limited to personnel who need the information to perform their job functions. Only users with proper permissions, roles, and security attributes are authorized to access the system. Each user is obligated to sign and adhere to a user access agreement, which outlines the appropriate rules of behavior tailored for FDNS-DS. The system administrator is responsible for granting the appropriate level of access. Furthermore, all employees are properly trained on the use of information in accordance with DHS policies, procedures, regulations, and guidance.

FDNS conducts annual security assessments of FDNS-DS in accordance with FISMA requirements. Furthermore, FDNS-DS complies with the DHS 4300A security guidelines, which provide hardening criteria for securing networks, computers, and computer services against attack and unauthorized information dissemination. Additionally, FDNS is subject to random Office of Inspector General (OIG) and/or any DHS assigned third-party security audits.

In keeping with the audit controls and role-based access safeguards established under the DHS SharePoint and Collaboration Sites PIA,[23] the FDNS SharePoint site has a designated site owner, or administrator, responsible for determining the user base and ensuring the site is only used for approved purposes such as internal collaboration and document and workflow management. The site owner ensures that only users with a verifiable need to know have access privileges to the information on the FDNS SharePoint site. The FDNS SharePoint environment includes a template with a "Sensitive Personally Identifiable Information Allowed" banner at the top of pages approved to manage and share sensitive PII. In addition, the FDNS SharePoint site follows the compliance restrictions placed on SharePoint usage by completing this PIA and the accompanying SORNs. FDNS regularly reviews the

[23] *See* DHS/ALL/PIA-037 DHS SharePoint and Collaboration Sites, *available at* www.dhs.gov/privacy.

information posted to the SharePoint site, and if inappropriate posting of PII is discovered, FDNS ensures its immediate removal from the site and reports the posting as a privacy incident.

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

USCIS employees receive the required annual Computer Security Awareness training and Privacy Act training. In addition, FDNS requires that all FDNS-DS users receive training in the use of FDNS-DS prior to being approved for access to the system. This training addresses the use of the system and appropriate privacy concerns, including Privacy Act obligations (e.g., SORNs, Privacy Act Statements).

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

Users receive access to FDNS records and FDNS-DS only 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 and privacy training requirements.

A user requesting access must complete and submit Forms G-872A and B, *USCIS and End User Application for Access*. This application provides the justification for the level of access requested. The requestor's supervisor, the system owner, and the USCIS Office of the Chief Information Officer will review this request; if approved, the requestor's clearance level is independently confirmed and the user account established.

Criteria, procedures, controls, and responsibilities regarding FDNS systems access are contained in the Sensitive System Security Plan for FDNS. Additionally, there are several department and government-wide regulations and directives that provide additional guidance and direction.

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?

MOAs/MOUs between USCIS and other components of DHS, as well as MOAs/MOUs between USCIS or DHS and other agencies, define information sharing procedures for data maintained by FDNS. MOAs/MOUs document the requesting agency or component's legal authority to acquire such information, as well as USCIS's permission to share in its use under the legal authority granted by the INA. All MOAs/MOUs have been reviewed by the program, USCIS Privacy Officer, and the DHS Chief Privacy Officer.

Responsible Officials

Donald K. Hawkins
Privacy Officer
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

APPENDIX A

Administrative Site Visit and Verification Program Load Balancing Utility (ASVVP Load Balancing Utility)

Summary:

FDNS is launching the ASVVP Load Balancing Utility which is a Microsoft Access data form linked to a secure SQL server database to collect receipt data and manage the case selection process. FDNS employees will manually enter the application receipt number, the date the application was adjudicated as "approved," the validity period of the application, and the beneficiary's work site address located within the file. Cases subject to review include all applications that FDNS currently conducts an ASVVP site visit and are considered relevant to the ASVVP project mission, by type of form, class preference, and other pertinent criteria.

The database will also contain tables that provide geographical connections between USCIS Field Offices and all zip codes throughout the U.S. and protectorates. The ASVVP Load Balancing Utility combines the geographical zip code/Field Office information with the zip code of the Work Site Address to pre-filter the eligible applications into groups based on proximity to a Field Office. Regional managers can then select a Field Office, and the utility will then present the total number of eligible records located within range of the selected Field Office. The regional managers will enter a number representing the estimated work load limit for the selected Field Office and submit a request for randomization. The utility will then randomly select the requested number of applications from the displayed list and provide an exportable workload list for the selected office. Each randomly selected petition will be flagged in the utility so it cannot be selected twice.

The spreadsheets derived from the utility will contain the field office identifier, the receipt number for the application, the approval and validity dates, and the work site address. This information will be attached to an email and sent via secure means (i.e., encrypted) to the Service Center Fraud Detection Operation (CFDO) units to be utilized by Service Center personnel in pulling the records that are to be entered into FDNS-DS under the existing FDNS-DS PIA.

The expected result of the use of this utility will be a level playing field that affords reasonable workloads to USCIS Field Offices while maintaining as much of the random selection process as possible.

This is a desktop type utility that uses non-sensitive data from recognized sources to enhance the workload balancing for the entire ASVVP. The overall benefit of this utility will be to enforce the stability and efficiency of the ASVVP.

Data Elements:

Data will include the application receipt number, the date the application was adjudicated as "approved," the validity period of the application, the beneficiary's work site address located within the file, and geographical Zip code/Field Office information.

Population:

Cases subject to review under ASVVP.

Privacy Mitigation:

Access to the ASVVP Load Balancing Utility is determined by the FDNS ASVVP program which approves access on an individual basis. User login information is recorded in the data structure and is used to validate access. Unless the user’s login information is validated, neither access to the SQL database nor the Microsoft Access front end is allowed. General users have read only access and there are a small number of manager level users. Manager level users access data based on their location only. The data are of limited scope. Users can only select and/or edit within regional/office profiles that are controlled by rigid filtering. No deletions are permitted except on request to the data managers.

APPENDIX B

Security Checks for Temporary Protected Status (TPS) Applicants

Background:

Pursuant to 8 U.S.C. § 1254a, the Secretary of Homeland Security may designate a foreign country for Temporary Protected Status (TPS) due to conditions in the country that temporarily prevent the country's nationals from returning safely, or in certain circumstances, where the country is unable to handle the return of its nationals adequately. USCIS may grant TPS to eligible nationals of certain countries (or parts of countries), who are already in the United States. Eligible individuals without nationality who last resided in the designated country may also be granted TPS. See DHS/USCIS/PIA-016 - Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3) for more information on the processing of benefits at USCIS.[24] USCIS first published this Appendix on September 11, 2013. USCIS is updating this Appendix to reflect the execution of a Memorandum of Agreement (MOA) regarding National Counterterrorism Center (NCTC) access, use, and retention of Yemeni TPS information.

The Secretary may designate a country for TPS due to the following temporary conditions in the country:

- Ongoing armed conflict (such as civil war);
- An environmental disaster (such as earthquake or hurricane) or an epidemic; or
- Other extraordinary and temporary conditions.

During a designated period, individuals who are TPS beneficiaries or who are found preliminarily eligible for TPS upon initial review of their cases (*prima facie* eligible):

- Are not removable from the United States;
- Can obtain an employment authorization document (EAD); and
- May be granted travel authorization.

Once granted TPS, an individual also cannot be detained by DHS on the basis of his or her immigration status in the United States. TPS is a temporary benefit that does not lead to lawful permanent resident status or give any other immigration status. However, registration for TPS does not prevent an applicant from:

- Applying for nonimmigrant status;
- Filing for adjustment of status based on an immigrant petition; and/or
- Applying for any other immigration benefit or protection for which you may be eligible.

TPS designation is time-bound and requires the Secretary to extend designation (re-designate) for a country's TPS status. Re-designation allows USCIS to accept new applications for TPS. Once granted TPS, an individual must re-register during each re-registration period to maintain TPS benefits. Please refer to the "Countries Currently Designated for TPS" for a full list of countries that have been designated

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

as TPS by the Secretary of Homeland Security and their effective dates.

Applicants for immigration benefits from USCIS, including TPS, receive background and identity checks as part of the adjudication process. Currently, all applicants for TPS receive a biographic check using the Customs and Border Protection's TECS, as well as a biometric check using the Federal Bureau of Investigation Next Generation Identification. In addition to these checks, USCIS conducts additional screening on individuals who may be eligible for TPS based off their country of citizenship or to stateless persons who last resided in the designated country. This additional check will be conducted by the Fraud Detection and National Security (FDNS) Division in conjunction with NCTC. FDNS facilitates the additional screening of TPS applicants; however, the Service Center Operations Program (SCOPS) manages the TPS adjudication process.

Screening of TPS Applicants from Designated Countries:

As part of its administration and enforcement of the Immigration and Nationality Act, USCIS reviews TPS applications for "inadmissibilities" under the Immigration and Nationality Act that may affect a TPS applicant's eligibility for the benefit. For example, USCIS's review for inadmissibilities includes national security and terrorism-related inadmissibilities as described in Sections 212(a)(3)(A), (B), or (F), or 237(a)(4) (A) or (B) of the Immigration and Nationality Act.

To support USCIS's identification of terrorism-related inadmissibilities, USCIS is partnering with the NCTC to determine if Terrorism Information exists in TPS applications from designated countries. Terrorism Information is defined as,

> (A)… all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to— (i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (iii) communications of or by such groups or individuals; or (iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and (B) includes weapons of mass destruction information.[25]

Using CLAIMS 3, USCIS extracts TPS applicant data and provide that list to the NCTC via encrypted electronic transmission in accordance with information security standards.[26] NCTC analyzes the TPS applicant data in conjunction with other data that NCTC holds, such as the Terrorist Identities Datamart Environment (TIDE), to determine if the TPS applicant data constitutes Terrorism Information.[27] In the event that NCTC identifies Terrorism Information associated with a TPS applicant,

[25] As defined in 6 USC § 485.

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

[27] TIDE is the central repository of identities information for known and suspected terrorists (KST). TIDE supports the U.S. Government's terrorist screening systems and the Intelligence Community's overall counterterrorism mission. The NCTC developed TIDE as part of the post-9/11 reform of the United States' watchlisting process, which consolidated multiple databases of international terrorist identities. The NCTC can perform batch queries of

USCIS reviews all available, relevant information and adjudicates the application pursuant to USCIS's legal authorities.

Data Elements:

USCIS provides NCTC with the biographic information derived from TPS applications, such as name, date of birth, country of birth, or other biographic data elements relevant to screening. DHS does not collect, generate, or retain any personally identifiable information beyond that which is collected, generated, or retained during the routine adjudication of TPS applications.

Population:

Currently, the population of individuals that are undergoing this screening are Syrian and Yemeni TPS Applicants. This PIA Appendix will be updated as additional countries are required to have this additional check.

Privacy Mitigation:

DHS and NCTC have entered a MOA that establishes the terms and conditions of NCTC's access, use, and retention of TPS information. The MOA limits NCTC's retention of TPS information so that NCTC only retains the information USCIS provides for analysis for as long as required to complete the mission. Under the MOA, NCTC may temporarily retain TPS information for 30 days. The purpose of this extended retention is to enable NCTC to continue to use the TPS Data in its counterterrorism analysis and to inform DHS of any subsequent terrorism-related concerns that may be identified after NCTC has performed the initial vetting of the TPS Data. The MOA also requires NCTC to delete the TPS information after it is no longer needed. After April 3, 2017, if the TPS information has not been identified as Terrorism Information, then NCTC will purge the records. If, during the course of the temporary retention period, NCTC identifies TPS information that is Terrorism Information, NCTC may retain, use, and disseminate the information consistent with its authorities.

The MOA also features protections against unauthorized dissemination of TPS information. Pursuant to the MOA, NCTC may disseminate TPS Data identified as Terrorism Information consistent with its authorities without the need for DHS approval, provided such dissemination is to other appropriate federal departments and agencies with counterterrorism responsibilities for counterterrorism purposes. NCTC may not otherwise disseminate TPS data absent written permission from DHS, including review and approval by USCIS, the DHS Privacy Office, Office for Civil Rights and Civil Liberties, Office of the General Counsel, and Policy Office.

TIDE and other classified holdings, to determine if Terrorism Information exists for a subject.

APPENDIX C

Form I-854, Inter-Agency Alien Witness and Informant Record

Summary:

The USCIS Fraud Detection and National Security Directorate (FDNS) Law Enforcement Support Operation (LESO) Branch adjudicates benefit applications and ancillary benefits, coordinates with USCIS field offices for various programs, generates notional documents for undercover operations, and provides advice on law enforcement and intelligence agency-sponsored immigration benefits programs. One of the roles of FDNS is to provide immigration assistance to law enforcement entities. The S nonimmigrant program falls under this responsibility.

Congress established the S nonimmigrant program as part of the Violent Crime Control Act of 1994. This program provides a nonimmigrant status for alien witnesses or informants who meet the requirements and are sponsored by law enforcement entities. The alien witness or informant may be eligible to receive S nonimmigrant status by: (1) providing critical and reliable information concerning a criminal or terrorist origination or enterprise; (2) willing to supply such information to law enforcement entities or court; or (3) showing his or her presence in the U.S. is essential to the success of a criminal investigation or prosecution of an individual involved in a criminal or terrorist organization or enterprise. Law enforcement agencies (LEA) use USCIS Form I-854, Inter-Agency Alien Witness and Informant Record, to bring alien witnesses and informants to the United States in an S nonimmigrant classification.

Form I-854 consists of two parts: the I-854A and I-854B. Form I-854A is used to place an alien in S nonimmigrant status while Form I-854B is used to recommend the alien for adjustment of status. Both parts are submitted by the sponsoring LEA to request inadmissibility waivers for the alien and as a supporting document when submitting an application for permanent residence on behalf of a witness or informant. The form is circulated through several entities for review and concurrence before reaching USCIS, starting with the sponsoring LEA, the alien, a United States Attorney's office, U.S. Department of State, and U.S. Department of Justice, Criminal Division, before finally reaching USCIS. Each of these entities provides its signatory endorsement, which is required under 8 CFR Part 214.2(t)(4). The concurrence of each entity is required in order to waive any inadmissibility. When Form I-854A reaches USCIS, the form and supporting documentation are presented to the Associate Director of FDNS and a decision is made to approve or deny the request. Upon USCIS approval of the status, Form I-854A and all documentation provided in support of the Form are placed in the alien's respective Alien File (A-File). USCIS provides an approval letter to the LEA and the applicant may choose to submit an I-765, Application for Employment Authorization.

FDNS reviews the Form I-854B in support of Form I-485, Application to Register Permanent Residence or Adjust Status. USCIS will then process the Form I-485 pursuant to USCIS adjudicator's standard operating procedures.

Data Elements:

USCIS may collect personally identifiable information (PII) about the alien witness or informant and the alien witness or informant's derivative family members in connection with a Form I-854 filling, including: name, alias, address, A-Number, I-94 number, current location of alien, marital status, date of birth, place of birth, nationality, occupation, date of last entry into the U.S., criminal history, FBI number, Social Security Number, passport number, travel document number, S-Visa number, country of issuance of passport of travel document, expiration date of passport or travel document, place of last entry, date of last entry into the U.S., current immigration status (if changing status), class of admission, country of origin, gender, and signatures. The Form only collects this information for alien witnesses and informants sponsored by a law enforcement entity, as well as any family members that may be deriving the benefit.

USCIS may collect PII about the LEA in connection with a Form I-854 filing, including: agent name, requesting LEA, address, e-mail address, phone number, fax number, and signature.

Population:

The form is used by LEAs to bring an alien witness and informants to the United States in an S nonimmigrant classification, change an existing nonimmigrant classification to an S classification or adjust an S nonimmigrant classification to lawful permanent resident status.

When completing the Form I-854A, LEAs must request one of the following classifications:

(1) S-5 nonimmigrant classification: For an alien who possessed and is willing to provide to the requesting LEA critical, reliable information on a criminal organization and who otherwise qualifies under section 101(a)(15)(s) of the Immigration and Nationality Act (Act) and 8 CFR 214.2(t).

(2) S-6 nonimmigrant classification: For an alien who possessed and is willing to provide information on a terrorist organization, who will be or is placed in danger as a result, and is eligible for an award under section 36(a) of the State Department Basic Authorities Act of 1956, 22 USC 2708(a), and who otherwise qualifies under section 101(a)(15)(S) of the Act and 8 CFR 214.2(t).

Qualifying relatives (spouse, married and unmarried sons and daughters, and parents) of the principal alien witness and informant may be included in a request for the S nonimmigrant classification.

Privacy Mitigation:

USCIS only collects a limited amount of PII in order to adjudicate this form. The information collected is pursuant to 8 U.S.C. § 1101(a)(15)(S). The information is only used for the purposes outlined on the form instructions.

USCIS ensures that the PII that is collected is accurate and complete as best practical, by collecting information directly from the applicant and/or LEA.

After USCIS processes this form, USCIS places it directly into the individual’s A-File. USCIS controls the subject’s A-File for 100 years from the date of birth, and then transfers the files to National Archives and Records Administration (NARA) for permanent retention pursuant to the approved retention schedule [N1-566-08-11]. The A-File is the only place USCIS retains the form.

APPENDIX D

Fraudulent Document Recognition Training

Summary:

The mission of U.S. Citizenship and Immigration Services (USCIS) Fraud Detection and National Security Directorate's (FDNS) is to determine whether individuals or organizations filing for immigration benefits pose a threat to national security, public safety, or the integrity of the nation's legal immigration system. FDNS supports USCIS's mission by enhancing USCIS's effectiveness and efficiency in detecting and removing known and suspected fraud from the application process, thus promoting the efficient processing of legitimate applications and petitions.

FDNS facilitates the Fraudulent Document Recognition Training to detect and deter fraud by recognizing fraudulent immigration documents as well as detecting impostors. This course trains USCIS personnel on how to identify types of counterfeit identification documents commonly used by terrorists, identification theft offenders, and illegal immigrants. Topics include how to identify immigration documents, specifically Permanent Resident Cards and Employment Authorization Documents (EAD), common document security features, photocopy examination of altered genuine documents, as well as a review on impostor detection.

The purpose of this Fraudulent Document Recognition Training course is to educate and enhance the FDNS employee's ability to identify and differentiate between genuine, counterfeit, and altered documents. The training allows FDNS personnel to determine what fraudulent documents look like and understand how fraudulent documents relate to immigration benefit fraud, issues of terrorism, and other national security issues. During the course of the training, the facilitator provides examples of both genuine and counterfeit documents to distinguish the difference between fraudulent documents and valid documents that have failing or worn features.

USCIS provides Fraudulent Document Recognition Training to USCIS personnel only; USCIS does not use a virtual training environment for this training. FDNS holds this training course in a classroom setting at a secured USCIS facility. The training consists of a PowerPoint presentation covering detection and examination of Permanent Resident Cards and EADs. Instructors share real immigration documentation obtained through fraud investigations or the administrative process to review security features of genuine, counterfeit, and altered documentation. However, there is no handout and students must return all training materials at the end of the training session. The PowerPoint is stored on the FDNS internal drive and the immigration documents are stored in a secured locked room. These training materials are restricted to those with a valid need-to-know.

FDNS will retain this presentation indefinitely and update it as appropriate to include new versions of cards and new fraud techniques employed by aliens to circumvent regulation.

Data Elements:

The training presentation and immigration documents may contain real and fraudulent information about individuals. Personally identifiable information (PII) from the Permanent Resident Card, EAD card, and photocopied documents may include: the individual's name, address, Social

Security Number, A-Number, date of birth, receipt filing number, photograph, country of birth, admission code, financial information, employment history, and education history.

Population:

Individuals who submitted fraudulent and altered documents to USCIS.

Privacy Mitigation:

FDNS provides Fraudulent Document Recognition Training to USCIS personnel with a need-to-know for training purposes. To prevent the risk of disclosing more information than necessary, FDNS minimizes the use of PII by removing unnecessary or irrelevant content from training materials that are not aligned with the objective of the training goals.

The electronic PowerPoint will be used as a part of this training. Access to the Fraudulent Document Recognition Training is restricted to employees with a valid need-to-know. The instructor will only use government-issued equipment to store and access this training. FDNS stores this presentation on a internal drive that is not accessible to users outside FDNS. FDNS will maintain security controls for any relevant materials.

FDNS stores the official physical records in a locked compartment and will not leave the records unattended. FDNS will store these records in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know, such as a locked room where a guard and card reader controls access. FDNS collects all original, fraudulent, or photocopied document examples provided during training at the end of the training session and stores them securely.

APPENDIX E

Southeast Region Immigration Services Officer Fraud Referral Intake Log (SER ADJ Fraud Referral Intake Log)

Summary:

FDNS created the SER ADJ Fraud Referral Intake Log to capture and track all incoming fraud referrals from U.S. Citizenship and Immigration Services (USCIS) Immigration Services Officers (ISO).

Southeast Region (SER) ISOs document suspected fraud and forward the file to USCIS Fraud Detection and National Security Directorate (FDNS) after a supervisor approves a case for further inquiry. FDNS documents all incoming fraud referrals from ISOs in the SER ADJ Fraud Referral Intake Log spreadsheet and creates a record in FDNS Data System (FDNS-DS).

FDNS reviews the referral for completeness and will either accept or decline the referral. If declined, the FDNS-DS record is “closed” and FDNS returns the Fraud Referral Sheet (FRS) to the referring ISO with an explanation of why FDNS declined the referral. If accepted, FDNS designates the case as accepted in FDNS-DS, conducts research and investigation, and refers prosecutable cases to Immigration Customs and Enforcement (ICE) officers.

Maintaining the SER ADJ Fraud Referral Intake Log allows FDNS to:

(1) Report Statistics

FDNS Immigration Officers (IO) use the information in the intake log to generate workflow production reports. Each FDNS office manually generates reports and each office captures these reports differently. The intake log allows FDNS offices to report the required numbers with consistency across the region.

(2) Conduct Training

FDNS IOs are responsible for training ISOs on how to refer actionable fraud cases and known fraud patterns and trends. The SER ADJ Fraud Referral Intake Log captures the reason FDNS declined a fraud referral, which assists FDNS to identify individual and group training needs.

(3) Complete the FDNS survey

SER FDNS requires all referrals returned to ISOs with findings must have a five question survey attached for ISOs to complete and return to FDNS. Capturing this data on the SER ADJ Fraud Referral Intake Log will assist FDNS to determine where the surveys were sent and if a response was received. It also allows FDNS to reach out to the ISO directly to request a completed copy of the survey.

(4) Meet ISO Period Performance Appraisals

Supervisory ISOs request the data from the SER ADJ Fraud Referral Intake Log for individual ISO fraud referral counts.

Data Elements:

This log maintains information related to the referral, and actions taken by FDNS and ISOs. Data may include:

Referral Information

- Date of fraud referral
- ISO First Name
- ISO Last Name
- Receipt Number

FDNS Action

- Date created in FDNS-DS
- FDNS-DS Number
- Whether the referral was accepted or declined
  - If declined, the reason it was declined
- FDNS findings

ISO Action

- ISO decision on petition/application
- Date ISO issued a Notice to Appear (if applicable)

Population:

Cases referred by ISOs to FDNS for fraud.

Privacy Mitigation:

Only FDNS personnel with a need-to-know may access the SER ADJ Fraud Referral Intake Log. Further, FDNS maintains the intake log on the shared drive with restricted access, and user login and password controls are in place to monitor usage. In addition, USCIS FDNS provides training to all individuals who will be using the log to confirm proper handling of the information that is maintained. Finally, all USCIS employees are required to complete annual privacy training, which trains employees on the appropriate handling, use, and dissemination of personally identifiable information.

APPENDIX F

Overseas Verifications

Background:

Overseas Verification (OV) is the verification of events, education, and work experience that occurred in a foreign country or the authentication of documents or information that originated overseas and relate to an individual's application or petition for immigration benefits. USCIS conducts OVs as part of the administrative investigation process.

The USCIS office responsible for administrative investigations is USCIS Fraud Detection and National Security Directorate (FDNS). FDNS performs administrative investigations to produce information that USCIS Adjudications Immigration Services Officers (ISO) may use to determine an individual's eligibility for an immigration benefit. FDNS ensures its administrative investigations are narrowly tailored to verify relationships that are the basis for an individual to receive an immigration benefit; to identify violations of the Immigration and Nationality Act; and to identify other grounds of admissibility or removability.

FDNS Immigration Officers (IO) receive written fraud, national security, and criminal referrals from Adjudications ISOs. FDNS IOs may also receive referrals or Requests for Assistance (RFA) from law enforcement partners, RFAs from other USCIS Directorates and Program Offices, or tip letters from the public. A FDNS IO performs systems checks and research on the subject of the referral. Then, the FDNS IO determines whether to take any further action or decline the referral. If the FDNS IO determines an administrative investigation is necessary, he or she performs further checks to verify information provided on, and in support of, applications and petitions.

A FDNS IO pursues an OV after exhausting all domestic resources, such as research in government and commercial databases, public record research, file reviews, telephone calls, site visits, interviews of witnesses, requests for evidence, and internal RFAs. To initiate the OV process, a FDNS IO completes and uploads an Overseas Verification Request (OVR) into the FDNS Data System (FDNS-DS) and selects the appropriate receiving Overseas Office (USCIS or Department of State (DOS)). FDNS-DS then sends an email to the designated Overseas Office to begin the OV. A USCIS or DOS employee working at an Overseas Office (Overseas Officer) conducts the verification of information or documents, including the verification of events, education, and work experience or the authentication of documents that originated overseas. Verification activities include:

- Phone, fax, e-mail, or internet verifications;
- Primary document examination and comparison against local repositories and databases;
- Targeted interviews;
- Consultation with other USCIS offices, DHS components, or DOS employees;
- Consultation with foreign governments;
- Diplomatic notes; and
- Administrative site visits.

In order to verify information associated with an application or petition, the Overseas Officer may contact:

- The individual;
- Third parties with knowledge about the case including joint sponsors or other persons associated with the filing;
- Educational, financial, and governmental institutions;
- Places of employment;
- Religious establishments; and
- Medical facilities.

Once the Overseas Officer has taken all necessary steps to verify the document or information, he or she will input the necessary information into FDNS-DS by completing a Report of Overseas Verification (ROV) template. The ROV must detail the nature of the OV, who conducted the OV, how the OV was conducted, and the findings of the OV. A supervisor will review the ROV prior to returning to the requesting officer. After approval from the supervisor, the Overseas Officer will upload the approved ROV and supporting documents to FDNS-DS. The Overseas Officer then sends an email via FDNS-DS to the domestic officer with the requested information.

Information Collected:

The information collected and retained in FDNS-DS as a result of an OV varies depending on the reason for completing the Overseas Verification. For example, an officer may suspect that an applicant's birth certificate is altered. Therefore, the officer would request for the Overseas Officer to investigate the authenticity of the applicant's birth certificate. Appropriate supporting documentation may include a certified copy of the birth certificate from the foreign entity or a letter indicating that the birth certificate in question was altered. The Overseas Officer verifies the supporting documentation that was received through the case.

Population:

USCIS applicants and petitioners who have submitted information to USCIS to receive an immigration benefit. In some cases, USCIS may not be able to verify documents or information domestically and may need to conduct an administrative investigation or verification overseas.

Privacy Mitigation:

There is a risk that USCIS may disclose information about certain applicants who are designated as special protected classes when conducting an OVR. USCIS employees and contractors are required to complete the annual Privacy Awareness Training, which identifies how to safeguard documentation, as well as identify the criminal and civil penalties associated with the unauthorized disclosure of this information. In addition, employees are also given training on special protected classes and how their information should be safeguarded and protected from disclosure.

There is also a risk that USCIS may collect more information than necessary or collect information on the wrong person, as part of an investigation. USCIS mitigates this risk by training employees to narrowly tailor OVRs and ensure the correct information is associated with the request and

ROV. Additionally, Overseas Officers only seek to verify items that the FDNS IO is requesting in the OVR. For example, if an FDNS IO requests verification on the legitimacy of a birth certificate, the Overseas Officer will conduct an investigation to confirm its legitimacy.

APPENDIX G

FDNS Tip Reporting Process

Background:

USCIS FDNS has a growing need for innovative ways to receive and evaluate information from the public and from other governmental entities concerning suspected fraudulent activities in order to effectively anticipate and reduce the impact of immigration fraud.

Currently, there is no clear avenue for the public to report suspected immigration benefit fraud to USCIS. When contacting the USCIS National Customer Service Center (NCSC) to report fraud, individuals are directed to call the U.S. Immigration and Customs Enforcement (ICE) hotline, the U.S. Customs and Border Protection (CBP) phone number, or to visit ICE and CBP webpages. The ICE Law Enforcement Support Center (LESC) previously reviewed the tips and forwarded those that may involve immigration benefit fraud to the USCIS Vermont Service Center (VSC) FDNS Office for further review, routing, and any action the local office deemed necessary. This often resulted in multiple entities having to handle and re-route misdirected correspondences causing unnecessary delays in the processing of time-sensitive information. In addition, there is no mechanism for the public to electronically submit information related to fraudulent activities directly to USCIS.

To actively engage the public in combating immigration benefit fraud, USCIS FDNS created a centralized process for the public to directly report suspected immigration benefit fraud to USCIS. This further aligns with USCIS' strategic goal to strengthen the security and integrity of the immigration system.

USCIS FDNS Tip Reporting Process:

Headquarters FDNS (HQFDNS) has created a mechanism that will centralize the process and identify USCIS as the point of contact for the public and other government agencies to report immigration benefit related tips. The USCIS public website and the NCSC now provide the public and other government agencies (OGAs) with a USCIS email address they can use in order to report tips of alleged fraud.

Individuals are now able to submit a tip to USCIS directly by emailing Reportfraudtips@uscis.dhs.gov or by visiting www.uscis.gov, where a link to the mailbox is provided. The webpage lists suggested fields the reporter should include that FDNS has deemed useful when processing the tip. The list serves merely as a suggestion, the reporter can include as much or as little information as they wish. Furthermore, USCIS collects information from the reporter on a voluntary basis.

Upon receiving a tip, HQFDNS is responsible for logging, vetting, tracking, analyzing the tips received to determine the quantity and quality of information received, and the potential for successful outcomes. The vetting process, including a search of government systems to identify fraud leads or obtain additional identifying information, determines whether or not the tip is actionable. HQFDNS also assesses the veracity of the tip during the vetting process. If HQFDNS deems the tip actionable, HQFDNS forwards the appropriate office having jurisdiction over the individual (e.g., FDNS Division in the respective field office, Service Center, Asylum or RAIO Office) for investigation.

FDNS documents the tip according to currently established policies, procedures, and practices including the Fraud Standard Operation Procedures (SOP) and the FDNS-DS User's Guide. FDNS documents the query on a designated Enterprise Collaboration Network (ECN) site and the Fraud Detection and National Security-Data System (FDNS-DS). Access to the ECN site and the fraud tip mailbox is limited to individuals assigned to process the emails for distribution to the FDNS Division in the field office responsible for processing the tip. HQFDNS will also use the information to develop reports and track trends or patterns. FDNS logs results of tips that are not actionable on the ECN site and are not forwarded to the respective field office. A copy of each tip is stored in the email archive (.pst) files as well as in the ECN for 15 years in accordance to the NARA Retention Schedule noted in the FDNS PIA dated July 30, 2012.

Information Collected:

USCIS collects fraud tips on a voluntary basis. The type of information collected for each case varies but may include:

- The type of tip being reported (e.g., marriage or employer fraud);
- Whether or not the tip was previously reported to another agency;
- Name of the business or person allegedly committing the fraud;
- Identifying information for the individual/company allegedly committing the fraud to include name, email, phone number, address, nationality, aliases, A-number, and/or date of birth
- Contact information of the person reporting the fraud including full name, email, phone number, and address.
- Any further information the person wishes to provide regarding the tip.

HQFDNS enters fraud tips into FDNS-DS and the ECN site, which are accessible only to authorized employees If FDNS deems a case inactionable, it is documented on the ECN site, but not entered into FDNS-DS.

HQFDNS employees are also responsible for forwarding the tips to the appropriate USCIS Office (Field Office, Service Center, Asylum or RAIO Office) having jurisdiction over the Subject or pending applications/petitions identified in the tips or other external agencies.

Population:

Any individuals or entities, reported by the general public or OGAs, as well as individuals suspected of committing immigration fraud.

Privacy Risks & Mitigations:

Privacy Risk: Because tips are reports of alleged illegal or otherwise suspicious activities, FDNS will not contact the reported individuals to verify their information. There is a risk that information provided about an individual in a tip may not be accurate because the information is provided by a third party and not the individual himself or herself.

<u>Mitigation</u>: During the course of an investigation into the tip, FDNS uses a variety of resources (government and open sources, as described in the PIA) to determine the accuracy and reliability of the tip information, including in some cases by conducting an interview with the subject of the tip. FDNS always investigates and verifies tips before USCIS uses the information as the basis for an adverse action against an individual.

<u>Privacy Risk</u>: There is a risk that USCIS may retain the tip information for longer than necessary.

<u>Mitigation</u>: USCIS retains the information in accordance with the NARA-approved retention schedule. USCIS retains FDNS-DS records for 15 years from the date of the last interaction between FDNS personnel and the individual, no matter the determination. FDNS retains this information because the information received regarding a case may not be actionable at the time of receipt; however, it may become pertinent at a later date. (e.g., Marriage fraud tip received after USCIS grants LPR status may not be actionable at the time of receipt but can be further investigated at the time the applicant attempts to remove conditions or naturalize).