Privacy Impact Assessment
for the

Fraud Detection and National Security Directorate

DHS/USCIS/PIA-044

July 30, 2012

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

Reviewing Official
Mary Ellen Callahan
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 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 Fraud Detection and National Security Directorate is responsible for detecting, deterring, and combating immigration benefit fraud. The United States Citizenship and Immigration Services is conducting this Privacy Impact Assessment to document and assess how the Fraud Detection and National Security Directorate collects, uses, and maintains personally identifiable information.

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efficient, and timely manner.[1] This information is also used to determine if and when those benefits should be rescinded or revoked.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, 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

[1] For more information about the USCIS adjudication process, please see "USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3)" and "USCIS Computer Linked Application Information Management System (CLAIMS 4)" PIAs at http://www.dhs.gov/privacy.

[2] Conference Report, Fiscal Year 2005 Appropriations Act.

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.

<u>*National Security Division*</u>

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.

<u>*Fraud Division*</u>

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 (RFAs)[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;
- telephone calls;

[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.

- 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 SORN. 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 may 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
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhswide_sharepointcollaboration.pdf

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 can use information found in open sources to formulate a Request for Evidence (RFE), for 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

[7] 8 CFR Part 103.2(b)(16).

[8] For further information, see the FDNS-DS PIA http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_fdns.pdf.

national security concerns were found, the information maintained may be used to demonstrate an 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.

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.

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

Concurrent with the publishing of this PIA, DHS is publishing an updated system of records notice of DHS/USCIS-005 Fraud Detection National Security Records, to clarify that the SORN covers both those 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. 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. 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 by completing this PIA and updating the DHS/USCIS-006 SORN.

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

Yes. The Retention Schedule for FDNS was approved on September 1, 2005. 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.

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[9] for more information on the various forms that cover the initial collection of information from the individual.

[9] See the CLAIMS 3 and CLAIMS 4 PIAs at www.dhs..gov/privacy for additional information on the forms individuals submit during the initial collection of information.

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;
- 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 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

- 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

- Customs and Border Protection (CBP) TECS;
- United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Automated Biometric Identification System (IDENT); and
- United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Arrival and Departure System (ADIS).

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 Department of State's Consular Consolidated Database (CCD) and other government databases when needed to address national security concerns and facilitate pilot programs.[10]

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.

[10] See Appendix A.

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 SORN.

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 system of records notice. 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.

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 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 SORN for FDNS records.

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 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 is not used consistently with its original purpose and authority.

Mitigation: Consistent with FDNS' 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 SORN.

Privacy Risk: There is a risk that use of commercial or public information, or information obtained through social media, may contribute to an erroneous adverse affect 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 sue of social media websites.

Privacy Risk: There is a risk that information contained within FDNS system will be shared outside DHS for a purpose incompatible with the original collection.

Mitigation: Information shared outside of USCIS is shared in accordance with departmental information sharing guidance and is consistent with the original collection of enhancing both national security and the integrity of the legal immigration system. Information is only shared outside of the Department consistent with applicable information sharing access agreements and Routine Uses documented in the published SORN.

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 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 system 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 SORN.

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 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. As part of the application process, applicants authorize USCIS to release any information provided, as needed, to other federal, state, local, and foreign law enforcement and regulatory agencies during the course of the investigation so that the immigration benefit eligibility determination can be made. This release includes sharing with FDNS, which has the dual mandate to enhance both national security and the integrity of the legal immigration system.

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, 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: The primary risk associated with retention is retaining the data 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 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 DHS/USCIS-006 FDNS-DS SORN (August 18, 2008, 73 FR 48231).

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 routine use I, which permits FDNS 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 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. This is 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 the 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. Otherwise, FDNS does not share its information. 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 SORN.

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 SORN, 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.

Privacy Risk: There is a risk of access and redress restrictions of law enforcement sensitive systems.

Mitigation: Access to the records contained in this system could potentially inform the subject of an investigation about actual or potential criminal, civil, or regulatory violations, or reveal investigative interest on the part of DHS or another agency. Furthermore, access to the records could permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, and avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities, and would impose an impossible administrative burden on investigative agencies. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security. Nonetheless, individuals may seek access to records maintained in FDNS-DS as outlined in the Record Access Procedures of the SORN. Requests for such access will be reviewed on a case-by-case basis.

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,[11] 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 SORN. 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.

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.

[11] See DHS/ALL/PIA-037 DHS SharePoint and Collaboration Sites
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhswide_sharepointcollaboration.pdf

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

____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

APPENDIX

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.[12]

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[13] 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.

[12] ASVVP site visits are currently conducted on: 1) pre and post adjudication religious worker cases; and 2) approved, post adjudication H-1B (non-immigrant, specialty occupation worker) cases.

[13] Currently, only the California and Vermont CFDOs process ASVVP cases.

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.