Privacy Impact Assessment
for the

Fraud Detection and National Security Data System (FDNS-DS)

DHS/USCIS/PIA-013(a)

May 18, 2016

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 (DHS), U.S. Citizenship and Immigration Services (USCIS), developed the Fraud Detection and National Security Data System (FDNS-DS) as the primary case management system used to record requests and case determinations involving immigration benefit fraud, public safety, and national security concerns. Since its initial deployment, USCIS has incorporated a new screening functionality into FDNS-DS, known as ATLAS, to more effectively identify and review cases involving fraud, public safety, and national security concerns.[1] USCIS is updating and reissuing the entire FDNS-DS Privacy Impact Assessment (PIA), originally published on June 29, 2008, to capture these updates.

Overview

Every year, U.S. Citizenship and Immigration Services (USCIS) receives nearly 6.4 million applications for immigration benefits or service requests. USCIS is committed to ensuring the integrity of the United States (U.S.) immigration system. An integral part of USCIS's delegated authority to adjudicate benefits, petitions, or requests, and to determine if individuals are eligible for benefit or services, is to conduct screenings (i.e., background, identity, and security checks) on forms filed with the agency. USCIS Fraud Detection and National Security Directorate (FDNS) developed the Fraud Detection and National Security – Data System (FDNS-DS) to record, track, and manage the screening processes related to immigration applications, petitions, or requests with suspected or confirmed fraud, public safety, or national security concerns. FDNS also uses FDNS-DS to identify vulnerabilities that may compromise the integrity of the legal immigration system.

The 2014-2018 Department of Homeland Security (DHS) Strategic Plan states that DHS will enforce and administer the nation's immigration laws by "ensuring that only eligible applicants receive immigration benefits through expanded use of biometrics, a strengthening of screening processes, improvements to fraud detection, increases in legal staffing to ensure due process, and enhancements of interagency information sharing."[2] Recent events highlight the importance of screening immigration benefit applicants for fraud, public safety, and national security concerns. Within FDNS-DS, FDNS developed a screening module known as ATLAS. ATLAS's event-based screening capability increases the timeliness and quality of fraud referrals. For the purpose of this PIA, the term FDNS-DS encompasses both the case management system and the screening module, ATLAS.

[1] ATLAS is not an acronym.
[2] Department of Homeland Security. "Fiscal Years 2014 – 2018 Strategic Plan."

FDNS-DS receives, tracks, and records information through the following processes: screening, referrals made to FDNS, administrative investigations, and through conducting studies related to benefit fraud and trends[3], as detailed below.

Screening and Referrals to FDNS

The types of screening performed on immigration forms vary by the benefit/request type. In general, USCIS conducts background checks[4] to obtain relevant information in order to render the appropriate adjudicative decision with respect to the benefit or service sought, identity checks to confirm the individual's identity and combat potential fraud, and security checks to identify potential threats to public safety or national security. Standard checks may include:

- Biometric fingerprint-based checks:
    1. Federal Bureau of Investigation (FBI) Fingerprint Check
    2. DHS Automated Biometric Identification System (IDENT) Fingerprint Check[5]
    3. Department of Defense Automated Biometric Identification System (ABIS) Fingerprint Check[6]
- Biographic name-based checks:
    1. FBI Name Check
    2. TECS[7] Name Check

USCIS uses several systems to support the checks identified above, which are described in detail in the Immigration Benefits Background Check Systems[8] and Customer Profile Management Service[9] PIAs, as well as the PIAs associated with USCIS's case management

[3] *See* DHS/USCIS/PIA-013-01 FDNS Program, *available at* www.dhs.gov/privacy, for more information on the administrative inquiry process, adjudication, and BFA Process. FDNS completes administrative investigations to obtain relevant information needed to render the appropriate adjudicative decision.
[4] During the adjudication process, USCIS conducts four different background checks, two biometric fingerprint-based and two biographic name-based, which are discussed in detail in the Immigration Benefits Background Check Systems (IBBCS) PIA. *See* DHS/USCIS/PIA-033 IBBCS, *available at* www.dhs.gov/privacy.
[5] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy.
[6] For certain benefit types in which the beneficiary has a higher likelihood of having previously been fingerprinted by the U.S. military, USCIS conducts checks against the Department of Defense's Automated Biometric Identification System, as described in the Customer Profile Management System (CPMS) PIA. *See* DHS/USCIS/PIA-060 CPMS, *available at* www.dhs.gov/privacy.
[7] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS), *available at* www.dhs.gov/privacy.
[8] *See* DHS/USCIS/PIA-033 IBBCS, *available at* www.dhs.gov/privacy.
[9] *See* DHS/USCIS/PIA-060 CPMS, *available at* www.dhs.gov/privacy.

systems. As mentioned in those PIAs, USCIS adjudications staff must query multiple systems, in some cases manually. Through the development of a screening module within FDNS-DS, known as ATLAS, the need to independently query each system is greatly reduced, thereby streamlining the screening process and limiting the privacy risks associated with using multiple systems. ATLAS interfaces with other systems in order to automate system checks and promotes consistent storage, retrieval, and analysis of screening results to enable FDNS to detect and investigate fraud, public safety, and national security concerns more timely and effectively. The specific system interfaces that enable screening through ATLAS are detailed at Appendix A.

Within FDNS-DS, ATLAS's automated, event-based screening is triggered when:

1. An individual presents him or herself to the agency (e.g., when USCIS receives an individual's benefit request form[10] or while capturing an individual's 10-fingerprints at an authorized biometric capture site, for those forms that require fingerprint checks);
2. Derogatory information is associated with the individual in one or more DHS systems; or
3. FDNS performs an administrative investigation.

ATLAS receives information from the individual's form submission and from the biographic and biometric-based checks listed above. That information is screened through a predefined set of rules to determine whether the information provided by the individual or obtained through the required checks presents a potential fraud, public safety, or national security concern. The rules help standardize how information is analyzed and help to detect patterns, trends, and risks that are not easily apparent from the form submissions themselves.

Previously, FDNS-DS received information primarily through manual referrals of cases from USCIS adjudications staff. Since the development of ATLAS, cases can now be referred to FDNS for administrative investigation in the following manners:

Referrals through System Generated Notifications (SGNs)

The screening process described above automates the process of referring cases to FDNS for review. Certain events, such as when USCIS receives a benefit request form or the 10-print capture of an individual's fingerprints at a biometric capture center, trigger rules-based screening. If the benefit request form or biometric capture matches a rule, ATLAS produces an SGN, which is elevated in FDNS-DS for manual review. Once an SGN is produced, a specially trained FDNS Officer, known as a Gatekeeper, conducts a manual review of the SGN for validity, determines whether it is "actionable" or "inactionable," and, if "actionable," triages the SGN for further action.

[10] *See* DHS/USCIS/PIA-061 Benefit Request Intake Process, *available at* www.dhs.gov/privacy.

If an SGN is "actionable," it enters the formal FDNS-DS case management process. An SGN found to be "inactionable" may be closed without further action. The SGN itself is not considered derogatory. SGNs help FDNS Officers to detect potential threats earlier in the immigration benefit application process, to demonstrate the fidelity of the individual's biographic and biometric information, and to identify discrepancies more efficiently.

Fraud Tip Referrals

Members of the public and other government agencies can voluntarily submit a fraud tip to USCIS directly by emailing ReportFraudTips@uscis.dhs.gov. In the future, a static page will be available at www.uscis.gov, where a link to the mailbox will be provided. The webpage lists suggested fields that FDNS has deemed useful when processing the tip. The list serves merely as a suggestion; a fraud or tip reporter can include as much or as little information as he or she wishes. More information about the fraud tip reporting process is described in Appendix H to the FDNS Directorate PIA.[11]

Upon receiving a tip, FDNS evaluates the tip to determine if it is "actionable" or "inactionable" for investigation. If FDNS deems the tip "actionable," FDNS manually inputs the information into FDNS-DS and prepares the tip for an administrative investigation.

Manual Referrals

USCIS adjudications staff can make manual referrals to FDNS through FDNS's Intranet Fraud Referral System (iFRS). Through this process, adjudications staff complete a fillable electronic form using the USCIS SharePoint Enterprise Collaboration Network (ECN).[12] FDNS Officers review the referrals and determine if the referral is "actionable" or "inactionable" and manually enter the information into FDNS-DS. If "actionable," FDNS prepares the referral for administrative investigation.

Administrative Investigations

If FDNS determines an administrative investigation is necessary, FDNS conducts further checks to verify information prior to an adjudicative decision on the immigration benefit or service requested, to include resolving any potential fraud, public safety, or national security concerns. In conducting an administrative investigation,[13] FDNS may perform one, or a combination, of the following:

- Research in Government and commercial databases and public records;

[11] *See* DHS/USCIS/PIA-013-01 FDNS Directorate, *available at* www.dhs.gov/privacy.
[12] *See* DHS/ALL/PIA-037 DHS SharePoint and Collaboration Sites, *available at* www.dhs.gov/privacy.
[13] *See* DHS/USCIS/PIA-013-01 FDNS Directorate, *available at* www.dhs.gov/privacy, for more information on FDNS administrative investigations.

- Internet searches of open source information;
- Searches of publicly available information, including, but not limited to, social media sites;
- File reviews;
- Telephone calls;
- Site visits;
- Interviews of applicants, beneficiaries, petitioners, and others;
- Requests for evidence;
- Administrative subpoenas;
- Requests for assistance from law enforcement agencies;
- Overseas verifications; and
- Referral to law enforcement agencies.

FDNS may perform administrative investigations or work with partner agencies, as appropriate, and ultimately produces findings to sufficiently inform adjudications.

Federated Immigration Screening and Application Report (FISAR)

The Federated Immigration Screening and Application Report (FISAR) within FDNS-DS is an advanced search functionality that allows FDNS-DS users to view the entire screening history on an individual, including records of standard checks, any SGNs produced by ATLAS that relate to the individual, and administrative investigations performed. If there are SGNs in the individual's screening history, the FDNS-DS user can easily determine the status of those SGNs (e.g., pending or triaged). The gatekeeping process described above provides manual oversight to ensure that SGNs produced by the system are valid and that they relate to the individual.

Enhanced Analytical Capabilities

FDNS enhanced ATLAS with analytical capabilities to enable users to more easily query and visualize data within the system and to identify individuals who are filing for immigration and naturalization benefits who may potentially be engaging in fraudulent behavior or pose a risk to public safety or national security. During the screening process, ATLAS analyzes the results of biographic and biometric checks, applies rules, and performs link and forensic analysis and entity resolution among data received from multiple systems. ATLAS assists in confirming individuals' identities when individuals are potentially known by more than one identity by comparing the identity information provided by the individual with identity information in other systems checked

against the background, identity, and security check process. As an example, ATLAS can determine if an individual has applied for benefits using multiple biographic identities or aliases. ATLAS also visually displays linkages or relationships among individuals to assist in identifying non-obvious relationships among individuals and organizations with a potential nexus to criminal or terrorist activities. The results of this analysis may be produced and elevated in FDNS-DS in the form of an SGN or obtained through FISAR.

ATLAS's analytical capabilities do not alter the source data. All legal and policy controls around the source data remain in place.

USCIS is continuing to enhance its screening processes by incorporating seven core capabilities into ATLAS: (1) Predictive Analytics; (2) Link and Forensic Analysis; (3) Unstructured and Structured Analytics; (4) Intelligent Investigative Case Management; (5) Operational Decision Management; (6) Information Sharing and Collaboration; and (7) Entity Analytics. Before new analytical capabilities are deployed within FDNS-DS/ATLAS, the USCIS Office of Privacy will review them to determine additional privacy requirements, which may include updating or re-issuing FDNS PIAs or SORNs.

Types of Information Collected and Stored within FDNS-DS

The following information is collected and stored in FDNS-DS:

- Information collected during screening (i.e., background, identity, and security check processes) to include information provided by the individual on a benefit request form, in response to a request for evidence, or during an interview; derogatory information received in response to checks; and audit trails or logs reflecting the history of checks conducted on the individual;
- Information collected during the adjudicative and administrative investigation process;
- USCIS investigative referrals to law enforcement agencies (LEA) of suspected or confirmed fraud, public safety issues, or national security concerns;
- Referrals and leads from other government agencies and LEAs related to individuals with an immigration history with USCIS;
- Information collected during response to a Request For Information (RFI) from law enforcement and intelligence agencies;
- Referrals from the public or other governmental entities or fraud case referrals from the Benefit Fraud Assessment (BFA) process ("other referrals");
- Information from cases that are selected for study of benefit fraud rates or trends;

- Adverse information identified by USCIS from applications, administrative files, interviews, written requests for evidence (RFE) or site visits; resolution of any of the above-described categories of adverse information; and
- Adjudicative summaries and decisions.

This PIA generally covers the privacy risks and mitigation strategies associated with the FDNS-DS system and its screening (rules-based referrals) and case management capabilities. USCIS will maintain operationally sensitive appendices to this PIA that will analyze privacy risks and mitigation strategies associated with enhanced analytical capabilities that have been approved for use within FDNS-DS.

The privacy risks and mitigation strategies associated with the overall administrative investigation process are described in the FDNS Directorate PIA. Additionally, other published USCIS PIAs available http://www.dhs.gov/privacy cover the benefit request intake process, benefit request form analysis and case management, as well as the collection of biographic and biometric information that is used as part of the screening process. These published PIAs provide an in-depth discussion of these separate processes and evaluate the privacy risks and mitigation strategies built into each process.

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 legal authority to collect this information comes from the Immigration and Nationality Act 8 U.S.C. Section 1101 *et seq*. In addition, the Secretary of Homeland Security in Homeland Security Delegation No. 0150.1 delegated the following authorities to USCIS:

> "(H) Authority under section 103(a)(1) of the Immigration and Nationality Act of 1952, as amended (INA), 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 Customs and Border Protection (CBP) or the CIS and make recommendations for prosecutions, or other appropriate action when deemed advisable."

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

Information collected, maintained, used, and disseminated by FDNS-DS is covered under the following SORNs:

- DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), August 8, 2012 (77 FR 47411)
  - Final Rule for Privacy Act Exemptions, August 31, 2009 (74 FR 45084)
- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, November 21, 2013 (78 FR 69864)

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

Yes. FDNS-DS was approved for entrance into the DHS Ongoing Authorization Program on August 26, 2014. A system privacy plan is pending the completion of this PIA.

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

Yes. NARA approved the FDNS-DS retention schedule, N1-566-08-18. FDNS will retain the records 15 years from the date of the last interaction between FDNS personnel and the individual for records maintained in FDNS-DS. Records related to an individual's A-File will be transferred to the A-File and maintained under the A-File retention period. USCIS maintains records on individuals and all of their immigration transactions and law enforcement and national security actions (if applicable), in the A-File. A-File records are permanent records in both electronic and paper form. USCIS transfers A-Files to the custody of NARA 100 years after the individual's date of birth, in accordance with N1-566-08-011.

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.

Almost all of the information within FDNS-DS is originally submitted on a benefit request form that is subject to the PRA. However, there are no forms associated specifically with the collection of information in FDNS-DS. Please see the benefit request PIAs and Appendices for a

comprehensive list of the various forms that cover the initial collection of information from the individual.[14]

Section 2.0 Characterization of the Information

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

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

Due to the nature of the information within FDNS-DS, FDNS-DS contains sensitive personally identifiable information (SPII). Depending upon the category of information being collected in or attached to an FDNS-DS record, the system may collect the following SPII:

Information about individuals may include, if applicable:

- Full Name;
- Alias(es);
- Physical and Mailing Addresses;
- Alien Number (A-Number);
- USCIS Online Account Number;
- Social Security number (SSN);
- Date of Birth;
- Nationality;
- Country of Citizenship;
- Place of Birth;
- Gender;
- Marital Status;
- Military Status;
- Phone Numbers;

[14] *See* DHS/USCIS/PIA-061 Benefit Request Intake Process, *available at* www.dhs.gov/privacy.

- Email Address;
- Immigration Status;
- Government-issued Identification (e.g., passport, driver's license):
  - Document Type;
  - Issuing Organization;
  - Document Number; and
  - Expiration Date.
- Signature;
- Other Unique Identifying Numbers (e.g., Department of State (DOS)-issued Personal Identification Number, ICE Student and Exchange Visitor Number, USCIS E-Verify Company Identification Number);
- Arrival/Departure Information;
- Immigration History (e.g., citizenship/naturalization certificate number, removals, explanations);
- Family Relationships (e.g., parent, spouse, sibling, child, other dependents) and Relationship Practices (e.g., polygamy, custody, guardianship);
- USCIS Receipt/Case Number;
- Personal Background Information (e.g., involvement with national security threats, criminal offenses, Communist party, torture, genocide, killing, injuring, forced sexual contact, limiting or denying others religious beliefs, service in military or other armed groups, work in penal or detention systems, weapons distribution, combat training);
- Medical Information;
- Travel History;
- Education History;
- Work Information (contact information, position and relationship to an Organization, degree(s), membership(s), accreditation(s), license(s) identification numbers);
- Work History;
- Bank account or financial transaction history;
- Supporting documentation as necessary (e.g., birth, marriage, or divorce certificates,

licenses, academic diplomas, academic transcripts, appeals or motions to reopen or reconsider decisions, explanatory statements, criminal history documents, and unsolicited information submitted voluntarily by the applicants or family members in support of a benefit request);

- Physical Description (e.g., height, weight, eye color, hair color, race, ethnicity, identifying marks like tattoos or birthmarks);
- Photographs from Government-issued Identification (i.e., passport, Driver's license, and other identification card);
- Relationships to petitioners, representative, preparers, family members, and applicants;
- Case processing information such as date applications were filed or received by USCIS, application/petition status, location of record, other control number when applicable, and fee receipt data;
- Organizations associated with applications, petitions or other requests (Place of business or place of worship, if place of worship is sponsoring the individual);
- Civil or criminal history information;
- Uniform resource locators (URLs)[15] or Internet protocol addresses;
- Biometric identifiers or associated biographic information (e.g., photographic facial image, fingerprints, Fingerprint Identification Number (FIN), Encounter Identification Number (EID), and signature);
- TECS, National Crime Information Center (NCIC), Federal Bureau of Investigation (FBI) Terrorist Screening Database, and any other data and analysis resulting from the investigation or routine background identity and security checks performed in support of the adjudication process; or
- Any other unique, identifying information.

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

Information in FDNS-DS is collected during the following processes: the screening (i.e., background, identity, and security check) process, referrals made to FDNS, administrative investigations, and to conduct studies related to benefit fraud and trends.[16] Much of the information

[15] The URL is the unique address for a file that is accessible on the Internet.
[16] *See* DHS/USCIS/PIA-013-01 FDNS Program, *available at* www.dhs.gov/privacy, for more information on the administrative inquiry process, adjudication, and BFA Process. FDNS completes administrative investigations to

collected in the FDNS-DS is taken from the benefit request form submitted to USCIS by the individual or an authorized representative or preparer, or from systems against which that data is screened during the screening process. USCIS may also collect information through interviews and site visits and record this into FDNS-DS. Interviewees may include current/past employers, family members, applicants, or other authorized representatives or preparers.

The information can be collected automatically or manually, as described below.

Automatic Collection

FDNS-DS's event-based screening capability through ATLAS is an automatic collection process that records certain information for review. Screening within ATLAS is triggered when:

1. An individual presents himself/herself to the agency;
2. Derogatory information is associated with the individual in one or more DHS systems; or
3. Administrative investigations are performed.

ATLAS queries internal and external systems automatically to obtain data relating to an individual's background, identity, and security check. ATLAS receives biographic data (e.g., name, date of birth, alias) associated with the individual's benefit request form from USCIS case management systems or biographic data associated with the individual's biometric capture at an approved biometric collection site (e.g., FIN, A-Number), which may be screened against data in IDENT,[17] TECS,[18] or the Terrorist Screening Database[19] and then against FDNS-DS's rules engine and analytical tools to produce SGNs.

In addition to the automatic collection that occurs during the screening process, FDNS-DS has a direct connection to the Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR)[20] to obtain CLAIMS[21] information about benefit request forms, applications, or petitions that can be used to automate the population of case information within FDNS-DS, such as A-Number. This helps to reduce the risk of error from manual data entry and to preserve the integrity of the information found in source systems.

---

obtain relevant information needed to render the appropriate adjudicative decision.

[17] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy, for more information.

[18] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS), *available at* www.dhs.gov/privacy.

[19] *See* Privacy Impact Assessment for the DHS Watchlist Service *available at* www.dhs.gov/privacy, for more information.

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

[21] *See* DHS/USCIS/PIA-016(a) CLAIMS 3, *available at* www.dhs.gov/privacy, for more information.

A comprehensive listing of source systems for this automatic collection is routinely updated at Appendix A.

Manual Collection

FDNS-DS users may query several DHS databases or systems to obtain information. Information gathered from these systems (e.g., dates of birth, SSN, country of birth, address) may be added to FDNS-DS. A complete list of DHS systems researched during this process is also included in Appendix A to this PIA.

Federal, State, and Local Government Sources

FDNS Officers may obtain information from various external sources, such as:

- Department of Labor
- Department of State (DOS)
- Social Security Administration (SSA) Electronic Verification of Vital Events (EVVE) [22]
- Federal Aviation Administration websites
- Intelligence and law enforcement communities
- State and local government agencies
- Local, county, and state police information networks
- State motor vehicle administration databases and websites
- Driver license retrieval websites
- State bar associations
- State comptrollers
- State probation/parole boards or offices
- County appraisal districts
- State sexual predator websites

As described in the FDNS Directorate PIA, FDNS receives information from external partners or sources during the administrative inquiry process and as part of referrals, requests for

[22] EVVE system allows verification of vital record information from the states, including birth certificates. *See* Electronic Verification of Vital Events Program Operations Manual System, *available at* https://secure.ssa.gov/poms.nsf, for more information.

assistance, or requests for information. The type of information collected depends on the specific context of a given case within FDNS-DS.

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

FDNS collects information throughout the course of recording, tracking, and managing the screening and administrative investigation processes related to immigration benefit requests forms, applications, or petitions. FDNS may obtain information from commercial sources or from publicly available information on the Internet. Examples of commercial or publicly available sources FDNS may access include, but are not limited to:

- Commercial data brokers (e.g., Choicepoint AutoTrackXP, Lexis/Nexis Accurint, Thomson Reuters CLEAR)
- General legal research sites (e.g., Legal Information Institute)
- Internet sites such as university websites and newspapers, news media websites, United Press International, Reuters, and foreign news media websites
- Various search engines (e.g., Ask, Google, Yahoo, REFDESK)
- Social media websites (e.g., Facebook, Twitter, LinkedIn, Pinterest, Google+)[23]

FDNS-DS enables Officers to note the exact URL and include attachments of any information collected from commercial sources or publicly available information.

FDNS uses these various commercial and publicly available sources to verify information provided by the individual, support or refute indications of fraudulent behavior, and identify any threat to public safety or nexus to known or suspected terrorists in the processing of their benefit request, consistent with authority granted by the Immigration and Nationality Act.[24] In addition, the Secretary has delegated USCIS the authority to investigate alleged civil and criminal violations of the immigration laws, not limited to alleged fraud with respect to applications or determinations.[25]

[23] FDNS Officers who seek to access, process, store, receive, or transmit PII obtained through the Operational Use of Social Media while conducting investigations are required to complete a "Rules of Behavior (ROB) for the Operational Use of Social Media." These ROBs ensure that users are accountable for their actions on social media, are properly trained, and aware of the authorized use of social media sites.
[24] 8 U.S.C. 1101 et seq.
[25] *See* Secretary of Homeland Security Delegation No. 0150.1, Section II (H) and (I), for more information.

Compiling this information and taking action to prevent potentially malfeasant and sometimes dangerous people from staying in this country supports DHS's mission of preventing terrorist attacks within the United States and reducing America's vulnerability to terrorism, while facilitating the adjudication of lawful benefit applications.

2.4 Discuss how accuracy of the data is ensured.

FDNS-DS relies on the accuracy of the information as it is collected from the source. As such, the accuracy of the information in FDNS-DS is equivalent to the accuracy of the source information at the point in time when it is collected into FDNS-DS. During this process, FDNS conducts data validation to ensure accuracy of the data.

FDNS Officers compare information obtained during the screening and administrative investigation processes with information provided directly by the individual (applicant or petitioner) in the underlying benefit request form or in response to Requests for Evidence or Notices to Appear, to ensure information is matched to the correct individual, as well as to ensure integrity of the data. As described above, the information contained in benefit request forms, applications, or petitions may be matched against public records, commercial data aggregators, and public source information, such as web sites or social media, to validate the veracity of information provided by the individual.

FDNS uses public source information only as means to verify information already on file with USCIS or identify possible inconsistencies. Due to the inherent data accuracy risks of relying on information from the Internet, USCIS requires that no benefit determination action can be taken based solely on information received from a public source. The information obtained from a public source must be corroborated with authoritative information on file with USCIS.

In the event FDNS Officers learn that information contained within other systems of records is not accurate, the Officer will notify appropriate individuals within the USCIS Records Office or the federal agency owning the data, who will facilitate any necessary notifications and changes.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk to individual participation because FDNS Officers rely on a considerable amount of information collected from external sources beyond what individual submitted on his or her benefit request form.

Mitigation: This risk is partially mitigated. FDNS collects information from a variety of sources to verify the information provided by individuals in the course of a review of possible fraud, public safety, and national security concerns. FDNS has determined that in order to have

the best evidence available to support the adjudication process, 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 cases of fraud, criminal activity, public safety, and national security concerns and sufficiently informs the adjudication of the benefit application. This risk is also partially mitigated in that individuals have the opportunity to provide information directly to USCIS throughout the adjudication process and through interviews, Requests for Evidence, or Notices to Appear.

Privacy Risk: Due to FDNS's reliance on external sources, including commercial sources, public sources, or social media, there is a risk that USCIS will obtain and rely upon inaccurate data.

Mitigation: The risk is partially mitigated in that FDNS considers information derived from sources other than the individual, but also exercises caution about the information's accuracy. Due to its inherent lack of data integrity, public source information is not used as the sole basis upon which to adjudicate an immigration benefit or request, investigate benefit fraud, or identify public safety and national security concerns. FDNS compares historical, biographical, financial, and personal information presented by the individual against third-party sources, whenever possible.

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.

Privacy Risk: Because FDNS-DS aggregates information from multiple source systems, there is a risk of data inaccuracy if the data in the underlying system(s) change.

Mitigation: As noted above, FDNS has policies and procedures in place to confirm the veracity of the data being relied upon in resolving potential fraud, public safety, and national security concerns. FDNS-DS also queries other systems in real time to receive the most timely and accurate data available from the source system. Finally, individuals have opportunities to provide information directly through the adjudicative process.

Privacy Risk: In some cases, FDNS-DS users enter information into the system manually. There is a risk of human error, which could result in FDNS relying on inaccurate data.

Mitigation: FDNS has a vested interest and responsibility to maintain the most accurate data possible since the information could be used in support of an adjudicative decision or in support of criminal investigations undertaken by law enforcement partners. FDNS Officers rely on multiple sources to confirm the veracity of the data and, if discrepancies are uncovered, will take necessary steps to correct inaccuracies.

Privacy Risk: There is a risk that search functions that previously could only have been performed through separate searches of individual systems or databases will allow FDNS-DS users (or users of other case management systems that receive data from FDNS-DS) to access to more data than is necessary to perform their specific roles.

Mitigation: This risk is mitigated in that FDNS-DS maintains strict access controls so that only FDNS-DS users with a role in investigating cases for potential fraud, public safety, and national security concerns have access to raw data retrieved as part of the screening process. FDNS-DS interfaces with other systems to help streamline the processes that FDNS-DS users currently perform manually, and its capabilities are designed to assist officers in obtaining information needed to confirm an individual's eligibility for the benefit or request sought while preserving the integrity of the legal immigration system. The output to other case management systems is reasonably tailored to provide adjudications staff with information relevant to making a determination on the benefit or request sought.

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

Mitigation: The risk is partially mitigated. In order to reduce the risk of new data being incorporated into FDNS that has not been reviewed for privacy and legal concerns, multiple layers of privacy and legal review have been built into FDNS's processes. The process is memorialized via the Overarching Integrated Project Team (IPT) Charter, which is in the approval process. Additionally, new sources are reviewed through the FDNS weekly Screening and Case Management IPTs with participation from the FDNS Privacy Advisor and USCIS Office of Privacy. FDNS must submit a privacy threshold analysis and receive approval from the DHS Privacy Office before adding any new data sources.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

FDNS-DS records, tracks, and manages the screening process, thereby increasing the effectiveness of the U.S. immigration system in combating benefit fraud, protecting public safety, identifying potential threats to national security, and identifying vulnerabilities that may compromise the integrity of the legal immigration system.

Screening

FDNS uses FDNS-DS to manage the screening (i.e., background, identity, and security check) process in support of the adjudication of USCIS benefit requests, in a pre-decisional and deliberative process. The information can be collected as a part of an automatic collection or manual collection, as described in Section 2.2.

FDNS uses commercial and publicly available sources, as well as information from other federal, state, and local government sources, to verify information provided by the individual/applicant or his/her petitioner or representative, support or refute indications of fraudulent behavior, and identify any public safety concerns or nexus to known or suspected terrorists in the processing of the individual/applicant's benefit request, pursuant to the Immigration and Nationality Act.[26]

Case Management

FDNS-DS performs case management by recording, tracking, and managing the processes associated with detecting fraud, egregious or non-egregious public safety, and national security concerns. FDNS-DS is the central repository for all data gathered during the processes of performing screening on benefit request forms or applications received, performing administrative investigations, and conducting studies of benefit fraud rates and trends.

Studies Related to Benefit Fraud and Trends

FDNS uses FDNS-DS data to produce studies related to benefit fraud and trends.[27] Identification of fraud patterns and trends support operational decision management and inform future rules-based referrals.[28]

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.

[26] 8 U.S.C. Section 1101 *et seq.*
[27] *See* DHS/USCIS/PIA-013-01 FDNS Program, *available at* www.dhs.gov/privacy, for more information on the administrative inquiry process, adjudication, and BFA Process. FDNS completes administrative investigations to obtain relevant information needed to render the appropriate adjudicative decision.
[28] *See* DHS/USCIS/PIA-055 SAS Predictive Modeling Environment, *available at* www.dhs.gov/privacy.

Yes. FDNS is incorporating predictive analytics into FDNS-DS to assist in prioritizing the workload. Predictive technology is applied to known derogatory holdings (e.g., background check results) in order to categorize information so that the cases most likely to result in a referral for criminal action are prioritized for the most immediate review. All cases, regardless of their priority, are reviewed manually by FDNS Officers.

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

Yes. FDNS-DS information is accessed by or shared with employees or contractors of DHS components on a need-to-know basis. Limited U.S. Immigration and Customs Enforcement (ICE) and CBP personnel have been granted read-only access to FDNS-DS. Information sharing includes tracking interactions with ICE to determine if further law enforcement activities should be pursued. ICE and CBP must request USCIS permission to share USCIS data with external third parties.

At the time of publication of this PIA, FDNS is also working with ICE to establish a connection to improve the quality and exchange of information with ICE, consistent with the joint USCIS/ICE anti-fraud strategy discussed in the FDNS Directorate PIA. Through this connection, FDNS-DS will share information with ICE on cases that may involve egregious public safety concerns or require further criminal investigation.

Furthermore, at the request of DHS, RFIs for national security purposes from external entities are coordinated through DHS Office of Intelligence and Analysis (I&A) Single Point of Service (SPS).[29]

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information contained within the FDNS-DS system is not used consistently with its original purpose and authority or that individuals may use the data inappropriately.

Mitigation: Consistent with FDNS's mission of detecting, deterring, and combating immigration benefit fraud, all information contained within FDNS-DS is used to identify and track possible benefit fraud, 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.

Consistent with USCIS and FDNS governance, user permissions are managed in a stringent manner to ensure users are only granted the privileges and access necessary to perform their job.

[29] *See* DHS/ALL/PIA-044 DHS Single Point of Service Request for Information Management Tool, *available at* www.dhs.gov/privacy, for more information.

User roles within the application will also be managed in a manner that is reflective of the need for more restrictive access. Training of users will also incorporate the appropriate use and access of data.

External users (i.e., CBP and ICE users) are granted read-only access to FDNS-DS only. USCIS shares FDNS-DS data with ICE, and in some cases with CBP, to determine if further law enforcement activities should be pursued. ICE and CBP must request USCIS permission to share USCIS data with external third parties. This ensures sharing is consistent with the routine uses allowable in the FDNS SORN.

Privacy Risk: There is a risk that SGNs may present FDNS Officers with results that may contain too many false positives, which may render the resulting data unusable or unreliable or unfairly subject individuals to further scrutiny.

Mitigation: An onboarding phase allows for a period of refining rules before they are deployed across FDNS. This onboarding phase consists of FDNS-DS users in a limited rollout receiving rule alerts through e-mail notifications.

USCIS continually tunes the rules to narrow the scope of information provided to FDNS Officers. Rigorous quality control and assurance procedures are used to adjust rules as necessary to reduce the potential for false positives. FDNS continually monitors and refines rules based on appropriate metrics. The SGN process also provides for a layer of human review to confirm SGNs are actionable prior to routing them for further case management activity.

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

Mitigation: Individuals that are listed within FDNS-DS have potentially engaged in activities that require further review for potential fraud, criminal activity, public safety, and national security concerns. However, the existence of a record in FDNS-DS is not in itself considered derogatory or a reflection on the individual's eligibility for a benefit, request, or service. In determinations when potential was not realized, cases are marked with "no fraud found." Statements of Findings (SOF) or assessments will contain a summary for adjudication's use.

Privacy Risk: For certain benefits or service requests, FDNS must share the results of background, identity, and security checks or other forms of screening with other USCIS case management systems in order to provide information in support of adjudications. There is a risk that data will be inaccurately copied or that it may be taken out of context.

Mitigation: The risk is partially mitigated in that FDNS-DS, as a standard practice with A-File handling, allows the ability to copy a non-changing SOF for adjudications. A SOF is an

unchangeable, PDF document in FDNS-DS. In response to manual referrals made to FDNS-DS, FDNS users will complete a SOF or assessment, when required. The SOFs or assessments are shared with adjudications staff. Adjudications staff are trained on how to interpret information in the SOFs or assessments and their relevance in adjudicating immigration benefits and also coordinate closely with FDNS.

In future releases, FDNS-DS will interface with USCIS immigration case management systems to fully automate the screening process, as well as provide the background, identity, and security check results either in the form of a hit/no hit response, a summary of past screening history, or some usable form, in order to provide timely, meaningful information to adjudicative staff. The responses sent to the case management systems will be tailored to present adjudication officers with information relevant to determining the individual's eligibility for the immigration benefit or service sought.

Privacy Risk: With automating the screening process, there is a risk of recurrent screening or vetting of individuals beyond the original purpose.

Mitigation: USCIS has established a robust governance structure to ensure that screening rules are compliant with all legal and privacy requirements. New rules undergo several layers of operational, legal, privacy, and policy review before they are presented to the Deputy Director, USCIS, for final approval. Through this process, FDNS ensures that all screening activity is properly vetted and falls within USCIS's authority. All screening methods deployed are tailored to provide information that is relevant to the adjudication of a particular benefit or immigration service request. USCIS may conduct screening in situations in which USCIS has the authority to rescind, revoke, or otherwise terminate, to issue a Notice to Appear (NTA), or to refer to another government agency for criminal/civil actions. When USCIS may no longer take action on a benefit, service, or request, the screening will cease.

Privacy Risk: There is a risk that FDNS-DS users will create ATLAS rules without going through the appropriate rules review process.

Mitigation: The governance process ensures that new rules are not created or implemented within the system without review from the appropriate stakeholders, including privacy and legal review. Implementation of rules and generation of SGNs are required to be in compliance with the Privacy Act of 1974, E-Government Act of 2002, Homeland Security Act of 2002 and all DHS privacy policies. Additionally, the capture, use, and disclosure of PII through the rules process must be pursuant to applicable system of record notices and available routine uses.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

In addition to the publication of this PIA, USCIS has previously published a programmatic PIA and SORN for the FDNS Directorate. FDNS-DS collects information from other USCIS systems, which also have their own PIAs and SORNs published on the DHS website.

All applications for benefits from USCIS have a Privacy Act Statement providing notice to the individual regarding the use and collection of the information and these forms state the that information may be used for fraud detection. USCIS forms also notify the individual that information provided may be checked for completeness, that certain background checks may be conducted, or that USCIS may request an interview or further evidence.[30]

When FDNS conducts interviews and site visits, FDNS Officers identify themselves and notify the individual or beneficiary of the reason for the interview or site visit. Notice is given to an individual'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?

USCIS benefit request forms require that an individual provide specific information that may contain sensitive PII. The failure to submit such information could impact the processing or adjudication of an application or petition and thus preclude the individual from receiving the benefit, request, or service. Therefore, through the application process, individuals have consented to the use of the information supplied in the benefit request form or application to determine their eligibility for the benefit, request, or service sought. Further, fraud assessments and background, identity, and security checks are required by regulation on all requests/applications filed with USCIS. Benefits, requests, or services cannot be granted until those checks are complete, and the information submitted is essential to the conduct of those checks.[31]

[30] Adjudicators are responsible for making decisions regarding granting benefits.
[31] As required by Title 8 U.S.C. § 1101 et seq.

USCIS provides notice to all individuals at the time of collection through a Privacy Act Statement on all USCIS forms. Individuals 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 individual's request.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk to notice that benefit requestors will not know that FDNS will collect publicly available information about them, including information posted on public social media websites and platforms.

Mitigation: The risk has been mitigated to the extent possible because USCIS provides notice to individuals through an (e)(3) statement, the source system PIAs, the FDNS Directorate PIA, this PIA, and the associated SORNs. USCIS also provides notice of its fraud detection and national security work through its public website.[32]

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

USCIS retains application information to assist in identifying individuals 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. Records related to a person's A-File will be transferred to the A-File and maintained under the A-File retention period (N1-566-08-11). Upon closure of a case pertaining to an individual, any information that is pertinent to the adjudicative decision (such as a SOF), whether there was or was not an indication of fraud, criminal activity, public safety and national security concerns, is transferred to the associated A-File.

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.

[32] *See* https://www.uscis.gov/about-us/directorates-and-program-offices/fraud-detection-and-national-security/fraud-detection-and-national-security-directorate

Mitigation: FDNS mitigates this risk by destroying FDNS-DS data in accordance with approved NARA records retention schedules. The 15-year retention schedule for FDNS data (N1-566-08-18) provides access to information that can be critical to research related to suspected or confirmed fraud, public safety, and national security concerns for individuals who may still be receiving immigration benefits or services. 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.

Privacy Risk: There is a risk that data will be retained in FDNS-DS longer than allowed by the original source system.

Mitigation: This risk is mitigated in that FDNS-DS retains data relevant to the background check/screening process and to cases of suspected or confirmed fraud, criminal activity, public safety and national security concerns. The system's master 15-year retention period is shorter than that of many USCIS case management systems from which application data is derived.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state, and local government; and private sector entities.

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

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. RFIs may be received from federal law enforcement agencies (e.g., Department of Justice (DOJ) FBI, DOS), the Intelligence Community, and authorized state or local law enforcement agencies who are parties to information sharing agreements managed by DHS. USCIS provides access to the requested data through direct user accounts or through copying of data to an electronic device or medium.

Requests for information are governed by the DHS/USCIS-006 Fraud Detection and National Security Records (FDNS) System of Records[33], the DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records[34], or in some instances, the originating

[33] 77 FR 47411 (Aug. 8, 2012).
[34] 78 FR 69864 (Nov. 21, 2013).

system of records notice for the underlying USCIS records, e.g., DHS/USCIS-007 Benefits Information System (BIS).[35] When covered by an applicable routine use and when appropriate, USCIS may share the sensitive 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 identity and security checks involving immigrant benefit fraud, criminal activity, public safety, and national security concerns.

Through direct user account access, DOS Bureau of Consular Affairs may view 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. 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, criminal activity, public safety, and national security concerns. In these cases, FDNS may proactively share information with other government entities as described under the FDNS and A-File SORNs.[36]

RFIs for national security purposes from external entities are coordinated through DHS I&A SPS. 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 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 applications for benefits. This is compatible with the original collection under the 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 the 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

[35] 73 FR 56596 (Sept. 29, 2008).
[36] *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 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, 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. FDNS also shares data internally via secure government networks.

A Memorandum of Understanding (MOU) between DHS and the FBI Terrorist Screening Center (TSC) for real-time screening against TSDB records also fully outlines responsibilities of the parties, security standards, and limits of use of the information, including re-dissemination.

A MOA between DHS and the National Counter Terrorism Center also fully outlines responsibilities of the parties, security standards, and limits of use of the information, including re-dissemination in accordance with the United States Attorney General Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information (March 22, 2012).

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

FDNS maintains a record of disclosure of FDNS-DS information provided outside of the Department in FDNS-DS. 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.

As mentioned in the FDNS Directorate PIA, FDNS may receive requests for assistance from external law enforcement partners. These requests are evaluated on a case-by-case basis, and disclosures must abide by all privacy laws and legal requirements. Some FDNS Officers are detailed to partner agencies to provide assistance as immigration subject matter experts. All FDNS Officers must abide by all privacy laws and legal requirements before sharing any immigration information. Disclosures made pursuant to these requests for assistance are tracked in FDNS-DS.

Further, at the request of DHS, Requests for Information for national security purposes from external entities are coordinated and tracked through the DHS I&A SPS process.[37]

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 to every agency in accordance with a routine use and 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.

[37] *See* DHS/ALL/PIA-044 DHS Single Point of Service Request for Information Management Tool, *available at* www.dhs.gov/privacy, for more information.

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 MOUs with federal and foreign government agencies. Finally, United States government employees and contractors must undergo annual privacy and security awareness training.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, or filing complaints.

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

Because FDNS-DS contains sensitive PII 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. When such a request is made, and access would not appear to interfere with or adversely affect the national or homeland security of the U.S. or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of USCIS, and in accordance with procedures and points of contact published in the applicable SORNs.

Individuals seeking to access information maintained by FDNS should direct their requests 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 Act Request" to ensure proper and expeditious processing. The requester should provide his or her full name, date and place of birth, and verification of identity in accordance with

DHS regulations governing Privacy Act requests (found at 6 CFR Part 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?

As stated above, individuals may use the Freedom of Information Act/Privacy Act process to request access to and correction of records maintained about them. The data accessed by FDNS-DS from underlying USCIS source systems may be corrected by means of the processes described in the PIAs and SORNs for those systems. In the event inaccuracies are noted, files and FDNS-DS records may 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, and by USCIS personnel who interact with individuals in the course of processing requests for benefits or services. Furthermore, this PIA and the respective SORNs serve as notice to individuals.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may be able to access, correct, or make amendments to records in the source systems, but may not be able to do so for their records maintained in FDNS-DS due to the Privacy Act exemptions claimed.

Mitigation: While FDNS maintains pre-decisional, deliberative information in FDNS-DS, individuals may still request access to records that USCIS maintains about them. Notice on how to file a Privacy Act request about records contained in maintained by FDNS is provided by this PIA and the FDNS SORN. Individuals can request access to information about them through the Privacy Act and 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

The following questions are intended to describe technical and policy based safeguards and security measures.

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

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-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. Finally, all employees are trained on the use of information in accordance with DHS policies, procedures, regulations, and guidance.

FDNS conducts continuous 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) or any DHS assigned third-party security audits.

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

FDNS-DS users receive the required annual Computer Security Awareness training and Privacy Act Awareness training. In addition, users receive training in the use of FDNS-DS prior to being approved for access to the system. The training addresses the use of the system and appropriate privacy concerns, including Privacy Act obligations (e.g., SORNs, Privacy Act Statements). FDNS Officers also have several mandatory, job-specific training requirements that include discussions on Privacy Act obligations and other restrictions on disclosure of information.

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-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 verified by their supervisor and the FDNS-DS business owner, and have successfully completed all required training.

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. Additionally the requestor signs the USCIS Rules of Behavior before access is granted. The requestor's supervisor and the FDNS-DS business owner will review this request; if approved, the requestor's access level is independently confirmed and the user account established.

Criteria, procedures, controls, and responsibilities regarding FDNS-DS systems access are contained in the Sensitive System Security plan for FDNS-DS. 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 and MOUs between USCIS and other components of DHS, as well as MOAs and MOUs between USCIS or DHS and other agencies, define information sharing procedures for data maintained by FDNS. MOAs and 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. All MOAs and MOUs must be reviewed by the program and all applicable parties.

Responsible Officials

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

Approval Signature

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

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

APPENDIX A

List of Systems of Records Researched during the Screening Processes and Tracked in FDNS-DS

Below is a list of systems, both internal and external, that exchange data with FDNS-DS, including those used to support screening through ATLAS.

U.S. Citizenship and Immigration Services (USCIS) Systems

- National Benefit Center Process Workflow Repository (NPWR)[38] to facilitate screening on certain form types being processed through the National Benefit Center, Background Check Unit;
    - **PIA:** TBD
    - **SORN:** TBD

- Service Center Computer Linked Application Information Management System (SCCLAIMS)[39] to facilitate screening on forms processed in Computer Linked Application Information Management System (CLAIMS 3);
    - **PIAs:**
        - FDNS Directorate[40]
        - CLAIMS 3[41]

- CLAIMS 4;
    - **PIA:** CLAIMS 4[42]
    - **SORN:** Benefits Information System (BIS)[43]

- Electronic Immigration System (ELIS);
    - **PIA:** ELIS[44]

[38] NPWR is covered under DHS/USCIS/PIA-016(a) Benefits Processing of Applicants other than Petitions for Naturalization (CLAIMS 3).
[39] SCCLAIMS is a mirror copy of CLAIMS 3 data.
[40] *See* DHS/USCIS/PIA-013(a) FDNS Directorate, *available at* www.dhs.gov/privacy.
[41] See DHS/USCIS/PIA-016(a) CLAIMS 3 and Associated Systems, *available at* www.dhs.gov/privacy.
[42] *See* DHS/USCIS/PIA-015 CLAIMS 4 and subsequent updates, *available* at www.dhs.gov/privacy.
[43] 73 FR 56596 (Sept. 29, 2008).
[44] *See* DHS/USCIS/PIA-056 USCIS ELIS *available* at www.dhs.gov/privacy.

- **SORN:** Benefits Information System (BIS)[45]

- Case and Activity Management for International Operations (CAMINO);
  - **PIA:** CAMINO[46]
  - **SORN:**
    - A-File, Index, and National File Tracking System[47]
    - Background Check Service[48]
    - Intercountry Adoptions Security[49]
    - BIS
    - Asylum Information and Pre-Screening (AIPS)[50]

- Refugees, Asylum, and Parole System and the Asylum Pre-Screening System (RAPS/APSS);[51]
  - **PIA:** RAPS/APSS[52]
  - **SORN:** AIPS[53]

- Marriage Fraud Assurance System (MFAS);
  - **PIA:** CLAIMS 3[54]
  - **SORN:**
    - A-File, Index, and National File Tracking System
    - Background Check Service
    - BIS

- Adoption Case Management System (ACMS);
  - **PIA:** Forthcoming ACMS PIA

[45] 73 FR 56596 (Sept. 29, 2008).
[46] *See* DHS/USCIS/PIA-051 CAMINO, *available* at www.dhs.gov/privacy.
[47] 78 FR 69864 (Nov. 21, 2013).
[48] 72 FR 31082 (June 5, 2007)
[49] 72 FR 31086 (June 5, 2007).
[50] 80 FR 74781 (November 30, 2015).
[51] *See* DHS/USCIS/PIA-027 RAPS/APSS, and subsequent updates, *available at* www.dhs.gov/privacy.
[52] *See* DHS/USCIS/PIA-027 RAPS/APSS, and subsequent updates, *available at* www.dhs.gov/privacy.
[53] 80 FR 74781 (November 30, 2015).
[54] See DHS/USCIS/PIA-016(a) CLAIMS 3 and Associated Systems, *available at* www.dhs.gov/privacy.

- **SORN:** Intercountry Adoptions Security[55]

- USCIS Lockbox[56] to retrieve data from digitized forms;
  - **PIA:** Benefit Request Intake Process[57]
  - **SORN:**
    - A-File, Index, and National File Tracking System
    - Background Check Service
    - BIS
    - Intercountry Adoptions Security
    - AIPS[58]
    - Collections Records--Treasury/Financial Management Service[59]

- Person Centric Query Service (PCQS) to retrieve status information from the Central Index System (CIS);
  - **PIA:** PCQS[60]
  - **SORN:** See PCQS PIA Appendices for associated SORNs

- National File Tracking System (NFTS) to retrieve the physical locations of A-files;
  - **PIA:** NFTS[61]
  - **SORN:** A-File SORN

- Customer Profile Management System (CPMS) to retrieve data associated with biographic and biometric screening.
  - **PIA:** CPMS[62]
  - **SORN:**
    - Background Check Service

[55] 72 FR 31086 (June 5, 2007).
[56] *See* DHS/USCIS/PIA-003(a) Integrated Digitization Document Management Program (IDDMP), *available at* www.dhs.gov/privacy.
[57] *See* DHS/USCIS/PIA-061 Benefit Request Intake Process, *available at* www.dhs.gov/privacy.
[58] 80 FR 74781 (November 30, 2015).
[59] Treasury/FMS.017 - Revenue Collections Records, 74 FR 23006 (May 15, 2009).
[60] *See* DHS/USCIS/PIA-010 Person Centric Query Service (PCQS), *available at* www.dhs.gov/privacy.
[61] *See* DHS/USCIS/PIA-032 National File Tracking System (NFTS) *available at* www.dhs.gov/privacy.
[62] *See* DHS/USCIS/PIA-060 Customer Profile Management Service, *available at* www.dhs.gov/privacy.

- Biometric Storage System[63]

Other Department of Homeland Security (DHS) Component System Interfaces

- DHS Automated Biometric Identification System (IDENT[64]) to retrieve data associated with biometric screening;
  - **PIA:** IDENT[65]
  - **SORN:** IDENT[66]

- U.S. Customs and Border Protection (CBP) TECS system, to perform screening, including checks against the Federal Bureau of Investigation, National Crime Information Center (NCIC);
  - **PIA:** TECS[67]
  - **SORN:** CBP TECS[68]

- CBP Automated Targeting System-Passenger (ATS-P) and UPAX;
  - **PIA:** ATS-P[69]
  - **SORN:** ATS[70]

- DHS Watchlist Service for real-time screening against Terrorist Screening Data Base (TSDB) records; and
  - **PIA:** FDNS WLS PIA Update[71]
  - **SORN:** DHS WLS SORN[72]

---

[63] 72 FR 17172 (April 6, 2007).
[64] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy.
[65] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy.
[66] 72 FR 31080 (June 5, 2007).
[67] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, *available at* www.dhs.gov/privacy.
[68] 73 FR 77778 (December 19, 2008).
[69] *See* DHS/CBP/PIA-006(b) Automated Targeting System (ATS), *available at* www.dhs.gov/privacy.
[70] 77 FR 30297 (May 22, 2012).
[71] DHS/USCIS/PIA-027(e) DHS Watchlist Service, *available at* www.dhs.gov/privacy.
[72] 81 FR 19988 (April 6, 2016).

- DHS Email as a Service (EaaS) Simple Mail Transfer Protocol (SMTP) server for email.
    - **PIA:** E-mail Secure Gateway[73]
    - **SORN:**
        - General Information Technology Access Account Records System (GITAARS)[74]
        - General Personnel Records[75]

Other DHS Component Systems Accessed (Manually)

- CBP Analytical Framework for Intelligence (AFI)
    - **PIA:** AFI[76]
    - **SORN:** AFI for Intelligence System[77]

- CBP Arrival and Departure Information System (ADIS)
    - **PIA:** ADIS[78]
    - **SORN:** ADIS[79]

- ICE Student and Exchange Visitor Information System II (SEVIS)
    - **PIA:** SEVIS II[80]
    - **SORN:** SEVIS[81]

- ICE ENFORCE Alien Removal Module
    - **PIA:** Enforcement Integrated Database (EID) [82]

[73] See DHS/ALL/PIA-012 E-mail Secure Gateway and subsequent updates, *available at* www.dhs.gov/privacy.
[74] 77 FR 70792 (November 27, 2012).
[75] 77 FR 73694 (December 11, 2012).
[76] *See* DHS/CBP/PIA-010 AFI, *available at* www.dhs.gov/privacy.
[77] 77 FR 13813 (June 7, 2012).
[78] *See* DHS/CBP/PIA-24 Arrival and Departure System (ADIS), *available at* www.dhs.gov/privacy.
[79] 80 FR 72081 (November 18, 2015).
[80] *See* DHS/ICE/PIA-001(a) Student and Exchange Visitor Information System II (SEVIS), *available at* www.dhs.gov/privacy.
[81] 75 FR 412 (January 5, 2010).
[82] *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID) and subsequent updates, *available at* www.dhs.gov/privacy.

- **SORN:** Immigration and Enforcement Operational Records System (ENFORCE)[83]

[83] 80 FR 24269 (April 30, 2015).