Privacy Impact Assessment
for the

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

July 29, 2008

Contact Point
Edward Murphy
Mission Support Branch Chief,
Fraud Detection National Security
U.S. Citizenship and Immigration Services
(202) 272-9574

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The United States Citizenship and Immigration Services (USCIS) has developed the Fraud Detection and National Security Data System (FDNS-DS), a case management system used to record, track, and manage immigration inquiries, investigative referrals, law enforcement requests, and case determinations involving benefit fraud, criminal activity, public safety and national security concerns. The FDNS-DS system is an upgrade of the Fraud Tracking System (FTS). The FTS PIA was published on June 24, 2005.

Introduction

The Office of Fraud Detection and National Security (FDNS) of the United States Citizenship and Immigration Services (USCIS) has developed the Fraud Detection and National Security Data System (FDNS-DS). FDNS-DS is a central repository that permits specially-trained employees to record, track, and manage the background check and adjudicative processes related to immigration applications and petitions (applications) with suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns, and cases randomly selected for benefit fraud assessments (BFAs). The system will also have the capability to track the following:

1. USCIS investigative referrals to law enforcement agencies (LEAs);
2. LEA referrals to USCIS concerning subjects with pending immigration benefit applications or petitions;
3. background check referrals and resolutions associated with suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns; and
4. any additional inquiries conducted in order to confirm that the information on file is correct.

FDNS has created FDNS-DS, a centralized data system, in order to increase the effectiveness of United States (U.S.) immigration system in identifying threats to national security, combating benefit fraud, and locating and removing vulnerabilities that compromise the integrity of the legal immigration system. With the implementation of FDNS-DS, USCIS's capabilities for detecting and tracking benefit fraud and other criminal activity—and conducting efficient and accurate background check resolutions and adjudication of national security cases will be increased,

In order to achieve the goals discussed above, FDNS-DS will store data related to immigration applications involving suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns. The data will include the results of required background checks conducted in connection with pending petitions/applications that results in subsequent inquiries conducted to resolve the background check results. FDNS-DS will also contain the following information related to cases involving suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns: USCIS investigative referrals to law enforcement agencies (LEAs) of suspected or confirmed fraud or other criminal activity; LEA referrals to USCIS related to pending applications; referrals to USCIS from the public or other governmental entities or fraud case referrals from the BFA process ("other referrals"); adverse information identified by USCIS from applications, administrative files, interviews, written requests for evidence (RFEs) or site visits; results of resolution of any of the above-described categories of adverse information; and adjudicative summaries and decisions.

As noted above, FDNS-DS will store information concerning cases randomly selected for BFAs and will track interactions with Immigration and Citizenship Enforcement (ICE) and other LEAs (e.g., the

Federal Bureau of Investigation [FBI], the Drug Enforcement Administration [DEA], and U.S. Customs and Border Protection [CBP]) in cases involving fraud or other criminal activity, and the Department of State in cases involving fraud related to selected types of visas for entry into the United States

Section 1.0 Information collected and maintained

1.1 What information is to be collected?

FDNS-DS will contain both personally identifiable information (PII) and non-PII. PII is any information that reveals, either directly or indirectly, an individual's identity. Both types of information will be obtained by means of USCIS's resolution and adjudication of cases involving suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns and from cases used in BFAs which are documented in FDNS-DS.

Depending upon the category of information being collected in or attached to an FDNS-DS record, the system may collect the following PII:

- Individual's name;
- Alias;
- Social Security Number;
- A-Number;
- Associated A-Numbers of close relatives and associates;
- Receipt Number;
- Address (home and business);
- Date and place of birth;
- Country of citizenship;
- Citizenship status;
- Gender;
- Telephone number(s);
- E-mail address;
- Place of employment and employment history;
- Organizations (Place of business, place of worship, if place of worship is sponsoring the applicant);
- Family lineage;
- Bank account information and/or financial transaction history;
- Marriage record;
- Civil or criminal history information;
- Uniform resource locators (URLs);
- Education record;
- Internet protocol addresses;
- Biometric identifiers (Photographic facial image, fingerprints, signature, etc);
- TECS, NCIC, and data and analysis resulting from the investigation or routine background checks performed as part of the adjudication process;
- or any other unique identifying number or characteristic.

FDNS-DS users will also have the capability to query previously entered data from cases to generate reports of cases matching the queried criteria. These reports will only contain data from FDNS-DS, and the query will not extend to other USCIS systems or cases outside of FDNS-DS.

1.2 From whom is information collected?

FDNS-DS is a case management system used to record, track, and manage immigration inquiries, investigative referrals, law enforcement requests, background checks, and case determinations. Information is collected from many different sources, including USCIS databases, other federal law enforcement systems, commercial data providers, state and local government databases, and public source information, such as newspapers and/or the internet.

DHS Sources of Information

Much of the information collected in the FDNS-DS is taken from the application/petition submitted to USCIS by the applicant/petitioner or an authorized representative. USCIS Immigration Officers (IOs), Immigration Analysts (IAs), and Intelligence Research Specialists (IRSs) may also collect information through interviews and site visits and input the information into FDNS. Interviewees may include, but are not limited to, current/past employers, family members, petitioners, or applicants.

DHS Databases

IOs, IA's and IRS may also query one of USCIS's general immigration processing databases. Information gathered from these systems (i.e. dates of birth, SSN, country of birth, address) may be added to FDNS-DS. These USCIS databases include:

- Computer-Linked Application Information Management System (CLAIMS) 3, which is used to process applications including, but not limited to, an Adjustment of Status (Green Card) and Temporary Protective Status (TPS); 62 FR 59734
- CLAIMS 4, which is used to process applications for Naturalization; 62 FR 59734
- Refugee Asylum Parole System (RAPS), which is used to process Asylum applications; 62 FR 59734 and
- Marriage Fraud Assurance System (MFAS), which is used for processing information relating to investigations of marriage fraud62 FR 59734.
- Background Check System (BCS) (71 FR 70413), USCIS' repository of background check requests and results.
- Central Index/A file, (72 FR 1755) the record that contains copies of information regarding all transactions involving an individual as he/she passes through the U.S. immigration and inspection process.
- Treasury Enforcement Communication System (TECS/IBIS) (66 FR 52984). FDNS officers may query Treasury Enforcement Communication System/Interagency Border Inspection System (TECS/IBIS) to obtain additional background information pertinent to the subject of the fraud investigation or background check.
- Customs and Border Protection Border Crossing Information System of Records. A new set of data that was previously covered by the TECS SORN which relates to crossing information.

FDNS-DS receives a nightly download of CLAIMS 3 data. FDNS-DS does not directly interface with any of the other USCIS databases identified above, and the information from CLAIMS 3 is not entered into FDNS-DS unless there is an identification of possible fraud.

USCIS, Fraud Tracking System (FTS). The USCIS Office of Fraud Detection and National Security (FDNS) developed FTS to decrease fraud in the immigration process. FDNS-DS encompasses the information that was previously maintained in FTS. FTS was a case management system used to track and control immigration fraud inquiries and investigative referrals. FTS allows USCIS users to conduct queries of the CLAIMS 3 database on a case-by-case basis to identify potentially fraudulent applications for immigration benefits. When an FDNS Officer identifies suspicious activities either from a tip or by searching the CLAIMS 3 database, a lead was opened in FTS and an FTS Identifier was created. The FTS Identifier was a unique system-generated number that was not specifically tied to an individual. This number was not recorded in the CLAIMS 3 system. The inquiry included investigative reports, administrative inquiry reports, or biographical information on an individual or a group of individuals. It was only after the completion of the inquiry that a note was made in CLAIMS 3 to record the results of the inquiry.

Non-DHS Sources of Information

IOs, IA's and IRS collect information throughout the course of recording, tracking, and managing the background check and adjudicative processes related to immigration applications and petitions (applications). Information may be obtained from publicly available information on the Internet, commercial and other government data sources such as Choicepoint AutoTrackXP, Lexis/Nexis Accrint, various local, county and state police information networks, various state motor vehicle administration databases, websites, driver license retrieval sites, state bar associations, the intelligence and law enforcement community, Department of Labor, Department of State, Federal Aviation Administration websites, Federal Express and DHL tracking, various state comptrollers, county appraisal districts, state probation/paroles, American Immigration Lawyers Association, Legal Information Institute, university websites, state sexual predator websites, news media websites, various search engines (i.e. Ask, Google, Yahoo), REFDESK (refdesk.com), United Press International, Reuters, and foreign news media websites.

Although no direct interface exists between FDNS-DS and these sources, USCIS IOs, IAs, and IRSs may enter information from these publicly available databases into FDNS-DS during the course of the administrative investigation, adjudication, and/or benefit fraud assessment.

1.3 Why is the information being collected?

FDNS-DS has been developed to streamline, in a centralized location, the identification and tracking of cases where there are national security, public safety implications, or indicia of fraud. Compiling this information and taking action to prevent potentially undesirable and often dangerous people from staying in this country supports two primary missions of DHS: preventing terrorist attacks within the United States and reducing America's vulnerability to terrorism, while facilitating the adjudication of lawful benefit applications. FDNS Officers use and track information from public sources, including commercial databases as a secondary source of information. It is used to verify existing information collected as part of the application process and to identify possible inconsistencies. Adverse action, such as denying a benefit, will not be taken based solely on the public source information.

1.4 How is the information collected?

FDNS-DS contains information collected throughout the following processes: administrative investigations, the process by which USCIS determines if fraud exists, adjudication process, and benefit fraud assessments[1]. FDNS-DS will also contain requests for assistance from law enforcement and intelligence agencies as well as USCIS referrals to law enforcement components such as ICE and the FBI.

1.5 What specific legal authorities/arrangements/agreements define the collection of information?

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).
>
> (I) 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 BCIS and make recommendations for prosecutions, or other appropriate action when deemed advisable."

1.6 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

USCIS FDNS-DS collects extensive information on individuals in the course of a review of possible national security concerns, public safety implications, or indicia of fraud. The information is maintained under strict access controls so that only those individuals within DHS with a need to know are able to access the information. Although a copy of data from other USCIS information systems is accessible through FDNS-DS, pertinent information from USCIS information systems will only be entered in FDNS-DS during background check resolutions or after fraud is detected.

While the collection of information presents inherent privacy risks, including the possible misuse and inappropriate dissemination of data, USCIS has implemented security measures in accordance with applicable laws and policies, including the DHS Information Technology Security Program Handbook, to mitigate these risks in the design of FDNS-DS. USCIS collects the required information that is necessary to record, track, and manage immigration inquiries, investigative referrals, law enforcement requests, and case determinations, and stores that information and the associated results in FDNS-DS.

The public source information is used as a means to verify information already on file with USCIS or identify possible inconsistencies. If the information is derogatory, pertinent to

[1] FDNS initiated a series of benefit fraud assessments (BFAs) beginning in January 2005. The purpose of the BFA is to determine the percentage and type of fraud that exists among certain immigrant and nonimmigrant petitions through a review of randomly selected applications for benefits. Information is collected and saved to the FDNS-DS as the system of record.

adjudication, and it will be used in the adjudication process, then by law we must notify the person and give them a chance to rebut.

Section 2.0 Uses of the system and the information

2.1 Describe all the uses of information.

Information will be used for recording, tracking, and managing the background check resolution and adjudicative processes related to immigration applications and petitions that generated the background check results. FDNS-DS includes tracking referrals to ICE and other law enforcement agencies (i.e. FBI, DEA, CBP) in cases that may warrant law enforcement action.

The information will be used to identify and track possible benefit fraud, criminal activity, public safety and national security concerns.

The public source information will be used to verify or identify inconsistencies with information already on file as part of an application with USCIS.

Not all applications require the submission of SSNs although some may, such as those submitted by USC sponsors. FDNS does not request the SSN number. However, if the immigration form that contained the SSN was provided it may be stored in FDNS-DS as part of the record.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

No, the system does not automatically analyze data to assist users in identifying previously unknown areas of note, concern, or pattern.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

The results of investigations will be compared with the underlying application or petition to ensure information is matched to the correct applicant/petitioner. The information contained in petitions and applications may be matched against public records, commercial data aggregators, and public source information such as web sites to validate the veracity of information provided by the applicant or petitioner.

Additionally, the public source information is used as means to verify information already on file with USCIS or identify possible inconsistencies. In order to mitigate the risk of inaccurate information being used, USCIS has in place the policy that no action can be taken based on information received from a public source. The information must be corroborated before it can be used to take action.

In the event FDNS officers learn that information contained within other USCIS systems of records is not accurate, the officer will notify appropriate individuals within the Office of Records or owning Federal agency who will facilitate any necessary changes.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above-described uses.

The information collected by USCIS IAs, IOs, Adjudication Officers, and IRSs will be recorded in FDNS-DS to track and manage the background check and adjudicative processes related to immigration applications and petitions that generated the background check results. In order to mitigate the privacy risk of inappropriate use of the information in FDNS-DS, USCIS developed FDNS-DS in accordance with DHS-approved security guidelines. Only users who have a need to know the information in the system can gain access to FDNS-DS, and their access to information contained within the system is restricted to what is necessary to perform specific job-related functions. These authorized users must go through an approval process and can only access FDNS-DS through DHS-approved equipment. Furthermore, users receive training on how to use FDNS-DS and restriction on sharing the information it contains. All users' actions are recorded and periodically audited by program management. Users have all been informed that inappropriate use of the system or information contained therein could lead to reprimands and job loss. All users also receive training on the proper handling of information in accordance with laws, regulations, and policy, including but not limited to the Privacy Act.

In order to improve the accuracy of the information, USCIS has developed policies and procedures for aggregating data from several different sources. This includes using both public source data and data from commercial aggregators and reviewing existing data in USCIS's files with information outside USCIS. If in the process of reviewing a file, inaccurate information is found, FDNS will contact personnel within the office of records who are authorized to make the changes.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

USCIS has proposed a retention period of 15 years from the date of the last interaction between FDNS personnel and the individual after which time the record will be deleted from FDNS-DS. Upon closure of a case, any information that is needed to make an adjudicative decision (such as a statement of findings report), whether there was or was not an indication of fraud, criminal activity, egregious public safety, and/or national security concerns, will be transferred to the A-File and maintained under the A-File retention period which is currently 75 years.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

No. However, USCIS has submitted an SF-115 for the FDNS-DS system and is awaiting NARA approval.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

The 15 year retention schedule is proposed to provide FDNS with access to information that is critical to the investigation of suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns.

Section 4.0 Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

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

Information contained in FDNS-DS may be shared with DHS Intelligence and Analysis (I&A) and may include name, date of birth, citizenship status and data and analysis resulting from the investigation or routine background checks (involving immigrant benefit fraud, criminal activity, public safety and national security concerns) performed as part of the adjudication process.

4.2 For each organization, what information is shared and for what purpose?

When fraud, public safety, or national security concerns are found as a result of an investigation or background check, and warrants law enforcement action, the information recorded in FDNS-DS is forwarded to ICE to determine whether further investigation or law enforcement action is warranted. If ICE accepts the investigation for law enforcement action, ICE will use the information collected in FDNS-DS to continue the investigation. ICE may in its discretion share information with other external law enforcement entities to include the Department of Justice.

Information shared with DHS Intelligence and Analysis (I&A) may include name, date of birth, citizenship status and data and analysis resulting from the investigation. Information will be shared with I&A if USCIS determines that there is a potential nexus to terrorism or that the information may have intelligence value. Pursuant to Section 201 of the Homeland Security Act, I&A is charged with the accessing, receiving and analyzing threats of terrorism against the United States.

4.3 How is the information transmitted or disclosed?

Information is transmitted over DHS secured, controlled networks utilizing DHS approved computers, services, and software in compliance with the requirements of the DHS 4300A Sensitive Systems Handbook. Only authorized users who need to know the information contained in FDNS-DS have access to information contained in the system.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Internal sharing of data is conducted over secured networks controlled by DHS utilizing DHS approved computers, services, and software. Only authorized users who need to know the information contained in FDNS-DS have access to the system. Authorized users must complete appropriate training prior to gaining access to the system. The FDNS-DS system owner must approve the individual applying for access and the user must have access to the USCIS intranet.

Section 5.0 External sharing and disclosure

5.1 With which external organizations is the information shared?

Pursuant to a Memorandum Of Understanding, authorized users in the Department of State's Consular Affairs Bureau have read-only access to FDNS.

In addition, USCIS receives and responds to requests for information in support of criminal and administrative investigations and background checks involving immigrant benefit fraud, criminal activity, public safety and national security concerns. The requests for information may be received from law enforcement agencies including the FBI and CIA, as well as Department of State, the intelligence community, the Director of National Intelligence, and authorized state or local law enforcement agencies who are parties to information sharing agreements managed by DHS.

5.2 What information is shared and for what purpose?

Department of State has read-only access to FDNS-DS to provide them with 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 Immigration and Nationalization Act. FDNS-DS may contain information relating to the following: fraud, public safety, and national security investigation activities and findings, immigration benefit application and petition information, and contact information for other investigating agencies.

In addition, FDNS on behalf of USCIS receives and responds to requests for administrative investigation and background checks involving immigrant benefit fraud, criminal activity, public safety and national security concerns. Information may be received from law enforcement agencies including the FBI and CIA, as well as Department of State, the intelligence community, the Director of National Intelligence, and authorized state or local law enforcement agencies who are parties to information sharing agreements managed by DHS. Depending on the particular situation, all or portions of the data collected through FDNS-DS may be shared with these agencies based on a need to know, to include where a potential for a nexus with terrorism exists. Any information will be shared in conformance with the Privacy Act of 1974, as amended and the published routine uses in the system of records notice.

5.3 How is the information transmitted or disclosed?

Information is transmitted over secured networks controlled by government agencies utilizing government-approved computers, services, and software.

Additionally, before information from FDNS-DS is accessed, transmitted or disclosed, the user or requestor must sign a Memorandum of Understanding (MOU) or other interagency agreement that will govern protection and usage of the information following DHS guidelines prior to the non-DHS agency obtaining access to FDNS-DS. Once the MOU or other interagency agreement is complete, the identified users of the agency must additionally complete access request forms (Form G-872O, Client Server Applications, Rules of Behavior, and Acknowledgement of Responsibility). All information transmitted or disclosed will be marked "For Official Use Only – Law Enforcement Sensitive" and contain the DHS logo, address and other appropriate USCIS markings. All US Mail or courier packages will be marked appropriately and sent via the appropriate government channels. Approved DHS communications systems will be used to transmit or disseminate FDNS-DS information. There are certain instances where an MOU or interagency agreement would not be required, but rather a written request pursuant to a published routine use. As an example, if Congress requests information on behalf of a constituent, DHS would provide the information.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

USCIS has entered into a Memorandum of Understanding with the Department of State providing them with read only access to the FDNS-DS. The MOU sets forth the nature of the information provided as well establishes standards for the safeguarding of DHS information.

5.5 How is the shared information secured by the recipient?

Information is shared with authorized personnel across networks controlled by the government using approved computer, services, and software in secure government facilities. The terms and conditions for the proper use of the data as well as the procedures for safeguarding the data are spelled out in the information sharing Memorandum of Understanding.

Any information that is extracted from the system will follow applicable laws and policies, including the DHS Information Technology Security Program Handbook. All information transmitted or disclosed will be marked "For Official Use Only – Law Enforcement Sensitive" and contain the DHS logo, address and other appropriate USCIS markings. All US Mail or courier packages will be marked appropriately and sent via the appropriate government channels. Approved DHS and other government communications systems will be used to transmit or disseminate FDNS-DS information.

In addition, government personnel and contractors must adhere to the OMB guidance provided in OMB Memoranda, M-06-16 "Protection of Sensitive Agency Information," dated June 23, 2006 setting forth the standards for the handling and safeguarding of personally identifying information. Contractors must also sign non-disclosure agreements.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

In compliance with the Federal Information Security Management Act (FISMA), OMB Policy, NIST guidance, and DHS/USCIS Policy requirements, all users of the FDNS-DS are trained on the Rules of Behavior and consequences for violating the rules. The Rules of Behavior must be read, acknowledged, and signed by FDNS-DS users prior to using the system. These requirements are incorporated into MOUs with both internal and external DHS agencies.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

The sharing of data with external agencies is conducted over government secure networks. All personnel within the receiving agency and its components are trained and authorized on the appropriate use and safeguarding of immigration data. In addition, each external agency involved has policies and procedures in place to ensure there is no unwanted dissemination of information. Any disclosure must be compatible with the purpose for which the information was collected, and only authorized FDNS-DS users with a need-to-know have access to information contained in the system. DHS information is covered by the third-party discovery rule, which precludes DHS information sharing without consent of DHS.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

- In addition to the publication of this PIA, a System of Records Notice (SORN) will be issued for FDNS-DS. Applicable SORNS for systems of records that may provide information to FDNS-DS include Computer-Linked Application Information Management System (CLAIMS) 3, which is used to process applications including, but not limited to, an Adjustment of Status (Green Card) and Temporary Protective Status (TPS); 62 FR 59734
- CLAIMS 4, which is used to process applications for Naturalization; 62 FR 59734
- Refugee Asylum Parole System (RAPS), which is used to process Asylum applications; and
- Background Check System (BCS) (71 FR 70413), USCIS' repository of background check requests and results.

- Additionally, 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.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

No. The personally identifiable information is collected from individuals who applied for immigration benefits and is stored in other USCIS case management systems prior to transfer to FDNS-DS.

USCIS benefit applications require that an applicant provide benefit specific information that may contain personally identifiable information. The failure to submit such information would prohibit USCIS from processing and properly adjudicating an application and thus preclude the applicant from receiving the requested benefit. Therefore, through the application process, individuals have consented to the use of the information supplied by the applicant or petitioner to determine their eligibility for immigration benefits. Further, fraud assessments and background checks are required by regulation on all applications or petitions filed with USCIS, benefits cannot be issued until those checks are complete, and the information submitted is essential to the conduct of those checks.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

USCIS benefit applications require an applicant or petitioner to supply accurate information to include personally identifiable information and other supporting documentation. Through the application process, individuals have consented to the use of the information. The information contained in USCIS is used solely for USCIS benefits determinations and any related law enforcement activities related to immigration law violations. Consent is given at the time of submission of the application or petition for benefits for this particular use. Individuals are directed to read the information on penalties that may result from the fictitious or fraudulent submission of data to DHS prior to completing their application for benefits. By signing, the individual certifies that, under penalty of perjury under the laws of the United States of America, that the petition and evidence submitted with it is all true and correct.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The collection of personally identifiable information is a required part of the application process, which must occur prior to the granting of an immigration benefit. The privacy risk associated with this particular collection of information is that the individual may not be fully aware that their information will be used to conduct an inquiry into benefits eligibility. In order to mitigate this risk, USCIS has provided a Privacy Act Notice on benefit application/petition forms, which states, "I certify under penalty of perjury under the laws of USA that the foregoing is true and correct. Furthermore, I authorize the release of any information from my records that the USCIS needs to determine eligibility for the benefit I am seeking". The form also contains a signature certification and authorization to release any information provided by an

applicant/petitioner. To further mitigate this risk, USCIS is issuing this PIA and the associated SORN.

Section 7.0 Individual Access, Redress, and Correction

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

For an individual to gain access to their USCIS record they can file a Freedom of Information Act (FOIA) or Privacy Act request.

USCIS may elect to withhold any related law enforcement sensitive information relating to a requestor, which could possibly compromise ongoing criminal investigations if released to the requestor, pursuant to the Privacy Act. 5 U.S.C. §552a(k)(2)

An individual may file a FOIA or Privacy Act request to view their USCIS record by submitting a written request to the following address:

National Records Center, FOIA/PA Office

P.O. Box 648010

Lees Summit, MO 64064-8010

Further information for FOIA requests for USCIS records can also be found at http://www.uscis.gov.

7.2 What are the procedures for correcting erroneous information?

If an individual would like to correct known erroneous information in their USCIS record, the individual can file a USCIS form directed at changing the specific erroneous information. For example, an applicant/petitioner can change their address by filing a Change of Address form (AR-11). After this form is processed the changes will reach FDNS-DS through one of the USCIS case management systems (see Section 1.2) and all relevant fields will be updated in FDNS-DS. If an applicant/petitioner believes their file is incorrect but does not know which information is erroneous, the applicant/petitioner may file a Privacy Act request as detailed in Section 7.1.

7.3 How are individuals notified of 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 benefit applicants/petitioners.

7.4 If no redress is provided, are alternatives are available?

Normal USCIS procedure for redress is provided to applicants/petitioners as outlined in Sections 7.1 and 7.2.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

The personally identifiable information data contained within FDNS-DS is obtained from other USCIS case management systems (see Section 1.2), and as such, individuals must address all information access rights to these systems. Previously established procedures for changing biographical information may be followed to correct known erroneous information, for example filing an AR-11 form to change an applicant/petitioner's address. If the applicant/petitioner suspects erroneous information but does not know which part of the information is incorrect, the applicant/petitioner can file a FOIA request as detailed in section 7.1.

USCIS may elect to withhold any related law enforcement sensitive information relating to a requestor, which could possibly compromise ongoing criminal investigations if released to the requestor, pursuant to the Privacy Act. 5 U.S.C. §552a(k)(2)

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system?

Access will be limited to authorized users of the system within DHS. Within this user group, FDNS-DS has four levels of access: Administrator, Super User, User, and Read-Only. External DHS users and selected categories of internals users will have restricted read-only access based on a need-to-know.

8.2 Will contractors to DHS have access to the system?

Yes, Contractors are used to maintain systems and provide technical support. All access to the FDNS-DS follows the access controls set up for access to USCIS computer systems. Access controls are applied to contractors and federal employees equally. In addition, all contractors undergo a background check including review of an individual's criminal history and credit history.

In compliance with the Federal Information Security Management Act (FISMA), OMB Policy, NIST guidance, and DHS/USCIS Policy requirements, all users of the FDNS-DS are trained on the Rules of Behavior and consequences for violating the rules. The Rules of Behavior must be read, acknowledged, and signed by FDNS-DS users prior to using the system. In addition, the underlying contracts contain non disclosure provisions binding on the contractor personnel with access to the FDNS-DS.

8.3 Does the system use "roles" to assign privileges to users of the system?

There are 4 levels of users for FDNS-DS:

- Administrator – System Administrators

- Super User – Users supporting application operational and training issues
- User – Immigration Officers and Intelligence Research Specialists
- Read-only – Users requiring read-only access

8.4 What procedures are in place to determine which users may access the system and are they documented?

A standard request form (G-872O) must be completed by each user and authorized by a supervisor in that department and by the system owner's representative.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

FDNS-DS maintains activity logs including transactions by user. Reports can be run to verify that a user's activity is consistent with their permissions. Access is granted based on a user's mission requirement and level of security clearance.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

FDNS-DS contains audit trail records to review and examine transactions. All FDNS-DS transactions are subject to routine monitoring and review to ensure that the original requests or results data are not lost, manipulated, and/or compromised in any manner. Further, all information will reside on a secured network and server; with access limited to authorized personnel only. Lastly, audit trails will be kept to track and identify unauthorized uses of system information.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

USCIS Immigration Officers, Adjudication Officers, and Fraud Detection National Security personnel receive privacy training at the Federal Law Enforcement Training Center during the course of instruction. USCIS employees and contractors will have access to FDNS-DS commensurate with the level of access required to perform their duties. These users will have previously undergone federally approved security clearance investigations and signed appropriate documentation to obtain the appropriate access levels. Federal employees and contractors are required to take annual computer security awareness training.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

The USCIS OCIO IT Security Office has developed and follows a security program compliant with the Federal Information Security Management Act (FISMA). The FDNS-DS has undergone the Certification and Accreditation (C&A) in compliance with FISMA and has been granted Authority to Operate (ATO) through April 2008.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Access and security controls have been established to mitigate privacy risks associated with authorized and unauthorized users, namely misuse and inappropriate dissemination of data. Authorized users will be broken into specific classes with specific access rights. Audit trails will be kept in order to track and identify unauthorized uses of system information. Further, FDNS-DS complies with the DHS security guidelines, which provide hardening criteria for securing networks, computers, and computer services against attack and unauthorized information dissemination.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

The system was designed with both commercial off-the-shelf (COTS) products and custom designed software, databases, and user interfaces.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

FDNS-DS developers followed the System Development Life Cycle security guidelines in the design and development of FDNS-DS. All documentation has been reviewed and approved by USCIS IT Security.

FDNS-DS developers followed the USCIS System Development Life Cycle 6.0 security guidelines in the design and development of FDNS-DS. All documentation has been reviewed and approved by USCIS Information Technology (IT) Security. Records will be attributed to the correct applicant/petitioner file by matching on multiple data points including A-Number, Receipt Number, Last Name, and Date of Birth. FDNS-DS data integrity checks were designed based on a detailed analysis of data sources (see Section 1.2) and specific data elements coming into FDNS-DS In addition to these integrity controls, the system was designed to acknowledge successful and failed data deliveries to ensure that data was never lost in transit.

FDNS-DS has been developed with industry standard interfaces that will allow for interface expansion. In the future, when an electronic system for automated sharing of information is developed, FDNS-DS will be able to easily interface with other systems.

9.3 What design choices were made to enhance privacy?

Read/write access to FDNS-DS is only available to USCIS employees and contractors with appropriate security and access controls. Read-only access will be granted to authorized personnel from ICE and DOS pursuant to Information Sharing MOUs with USCIS. The general public will not have access to the system. Protection and integrity of data, security, and privacy are of paramount concern. Information in this system is safeguarded in accordance with applicable laws and policies, including the DHS Information Technology Security Handbook. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include restricting access to authorized personnel who have a need-to-know, using locks, and password protection identification features. The system is also protected through a multi-layer security approach. The protective strategies are physical, technical, administrative and environmental in nature and provide access control to sensitive data, physical access control to DHS facilities, a confidentiality of communications, authentication of sending parties, and personnel screening to ensure that all personnel with access to data are screened through background investigations commensurate with the level of access required to perform their duties.

The system will provide more efficient management of the USCIS benefits eligibility process by consolidating all of the tracking to a single system. The ability to track data and user activities through audit logs on a consolidated system is far easier and provides better accountability than multiple systems can provide.

Conclusion

As an organization, both USCIS and the FDNS are committed to the safeguarding of personally identifiable information. FDNS-DS was designed to facilitate USCIS fraud, public safety, and national security case management. The FDNS-DS has both technical and policy safeguards in place to protect information processed by the system. FDNS has implemented and enforces operational controls not only in terms of the system but for paper files and personnel as well. Routine audits of the use of personal information are conducted.

The ways in which FDNS-DS addresses privacy concerns include, but are not limited to:

- Granting access to pre-approved USCIS employees and contractors;
- Auditing transaction records to ensure that requested information and result data are not manipulated or compromised;
- Providing FDNS-DS users with training that addresses privacy concerns; and

FDNS-DS is a multi-phased project and is currently in its second phase. As future phases are developed, this PIA and associated SORN will be revised to address those updates.

Responsible Officials

Edward Murphy
Mission Support Branch Chief, FDNS
U. S. Citizenship and Immigration Services
(202) 272-9574

Approval Signature

Original signed and on file with the DHS Privacy Office.
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security