Privacy Impact Assessment
for the

National File Tracking System (NFTS)

October 5, 2010

Contact Point

Donald K. Hawkins
Privacy Officer
US Citizenship and Immigration Services
(202) 272-8000

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The United States Citizenship and Immigration Services (USCIS) is preparing this Privacy Impact Assessment (PIA) for the National File Tracking System (NFTS). NFTS is an automated file-tracking system used to maintain an accurate file inventory and track the physical location of files. This system facilitates USCIS's ability to efficiently manage and streamline access to the millions of immigration files under its control. USCIS is conducting this PIA to document, analyze and assess the current practices with respect to the personally identifiable information (PII) NFTS collects, uses and shares.

Overview

USCIS, a component of the Department of Homeland Security (DHS), is responsible for administering and processing applications for all immigrant and non-immigrant benefits. To document the application process, USCIS creates the following files for each applicant (hereinafter referred to as *immigration files*) and an associated tracking number:

- Alien File (A-File) - files created for aliens seeking immigration benefits (i.e., lawful permanent resident, naturalization), aliens who illegally entered the U.S., or other individuals subject to the provisions of the Immigration and Nationality Act (INA);
- Certificate Files (C-Files) - files created for aliens naturalized prior to April 1, 1956;
- Receipt File – files created for both immigrant and nonimmigrant benefit applications. The receipt files for immigrants benefit applications will eventually be consolidated into an A-File;
- Temporary File (T-File) - temporary files created to store documents when the A-file is in another office location. When the office receives the A-File, the documents are merged with the A-File.
- Work Files (W-File) - files created to place copies of original documents from the A-file. Work files to be used for note taking and writing drafts. Drafts are then finalized and placed in the A-File.

The associated number with the above are referred to as "primary tracker numbers" for the remainder of this document. Customs and Border Protection (CBP), which performs the border enforcement and inspection processes, and the Immigration and Customs Enforcement (ICE), which performs the investigatory, deportation, and immigration court functions, also use the immigration files, especially the A-File. Although all three components, collectively known as the *Tri-Bureau*, use the immigration files in the course of performing their missions, USCIS is the custodian of these files.

The USCIS Records Division stores more than seventy million existing immigration files. The Records Division has over 150 File Control Offices (FCO) co-located with CBP and ICE worldwide. To ensure the proper handling and monitoring of its immigration files, USCIS created NFTS, a file-tracking system. NFTS is a web-based application that allows DHS to track and log the movement of paper-based immigration files in a centralized database, and provide timely and accurate access to the immigration file location. This system facilitates USCIS' ability to efficiently manage and streamline access to the millions of immigration files under its control. NFTS was built prior to the enactment of the E-Government Act. The system has undergone substantial changes since its development, which triggered the publication of this PIA.

When a user requires the A-File, the user goes to Central Index System (CIS) [1] and requests the file. CIS has a direct interface with NFTS, and receives the following information from it on the applicant: full name, the primary tracking number (the alien number (A-Number)) and date of birth. NFTS collects the following information directly from individual system users: system user's full name, office location, and responsible party code (RPC), which relates to either a system user or file shelf location and the immigration file's status (i.e., retired, record-in-use), and the last transaction (i.e., charged-out, received, in-transit). NFTS maintains this information in order to control the inventory of all files, query the file location, manage the request and transfer of files between offices and to/from the FCOs, provide reports to support management and cleanup efforts, and gather statistical information to improve the records processes. NFTS does not store a digitized copy or the entire content of the immigration files.[2] When the FCO receives the request for the A-File, the A-number and the person's full name and date of birth are printed on the pull ticket so that the FCO can verify the correct A-File is being pulled.

When a user requires any file other than the A-File, he must go into NFTS directly and using the primary tracker number, submit a request for the File. The pull ticket only has the primary tracker number and no other information.

NFTS has near real-time interfaces with National Archives and Records Administrations (NARA) Central Information Processing System (CIPS), system, thus increasing processing accuracy and efficiency for locating retired files.

NFTS also interfaces with several other USCIS systems in order to update the location of files for improved processing and efficiencies.

Tri-Bureau may assign A-Numbers to immigrants and non-immigrants. USCIS assigns an A-Number or one of the other immigration related numbers when an individual applies for a USCIS benefit. For example, USCIS creates an A-File when an individual applies or petitions for long-term or permanent USCIS benefits. CBP and/or ICE create an A-File in relation to pending enforcement actions. CBP and ICE assign A-Numbers to persons entering the United States illegally. USCIS Records Office distributes files with unassigned A-Numbers, sometimes referred to as "empty jackets," to the CBP and ICE. The employee assigns an A-Number to an applicant using an "empty jacket". Within 72 hours of assigning an A-Number, Tri-Bureau employees provide the USCIS records office with either the physical file or the documents used to initiate the file in cases where they need to keep the actual A-File. The USCIS records office updates the CIS with biographic information and NFTS with A-Number and file location manually.

Any one of the Tri-Bureau may need the physical file to adjudicate a benefit or review a case. NFTS is used to locate the physical file. To identify the FCO for the location of the A-File, users submit a request through CIS. The user submits the request and CIS interfaces directly with NFTS to determine the exact A-File location and request the file. The office where the A-File is located receives a pull ticket with the file number, which indicates which office is requesting the A-File. The user who has the file puts the pull ticket on the file and a mail person has the A-File delivered to the records department to update NFTS properly and then sends it to requesting office.

Authority for maintaining this system is derived from 8 USC §§ 1101, 1103, 1304 et seq., and 1360 and includes definitions, powers, and duties of the Secretary of Homeland Security.

[1] Please see the USCIS Central Index System PIA at: www.dhs.gov/privacy.
[2] Digitized A-Files are maintained and stored in the Enterprise Document Management Service (EDMS).

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

NFTS collects and uses information pertaining to the applicant, system user, and immigration file.

Applicant Data

NFTS maintains the following data elements on each applicant: full name, date of birth, and primary tracking number (immigration file numbers, such as, A-number, C-number, receipt number, T-number, and W-number). The primary tracking number is used to retrieve the transaction record pertaining to the immigration file. The general user is not able to see the applicant's information beyond the primary tracker, but it is used in the background to verify the correct information is pulled for the pull ticket.

Immigration File Tracking Data

USCIS uses the immigration file tracking data to locate files within the Tri-Bureau's and NARA. Data elements include: FCO location, RPC, status of the file (i.e., Retired, Records-In-Use), and last transaction (charge-out, received, in-transit) with time stamp.

System User Data

USCIS uses the system user data to identify the user updating NFTS. System user data includes: user ID, last name, first name, and business phone number.

1.2 What are the sources of the information in the system?

NFTS receives a feed from CIS for applicant data for A-files and receives a feed from Computer-Linked Application Information Management System (CLAIMS 3 and CLAIMS 4)[3] for receipt files.

System users create the Immigration file tracking data as they use the system to request and receive files.

Individual users provide the user information.

[3] Please see the USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum PIA for CLAIMS 3 and the Computer-Linked Application Information Management System PIA for CLAIMS 4 at: www.dhs.gov/privacy.

1.3 Why is the information being collected, used, disseminated, or maintained?

The information in NFTS is used to facilitate USCIS's ability to track the location of files in its inventory and the movement of files within the Tri-Bureau and locate retired files that have been sent to NARA.

1.4 How is the information collected?

NFTS receives limited data feeds directly from CIS, CLAIMS 3 and CLAIMS 4. Information is also received manually by scanning the barcode on the physical file to an updated location based on the actions of the user.

1.5 How will the information be checked for accuracy?

USCIS staff conduct audits of the physical location of files to validate the information in the NFTS database. The USCIS Records Operations Handbook requires at least one audit per year for each FCO and most offices conduct roving audits throughout the year. On a daily basis all offices manage NFTS reports for file accountability and if a file is found in an inaccurate location, the location information is updated to the correct location. USCIS records users verify and correct the FCO contact information, as necessary, through NFTS.

Additionally, all NFTS user accounts are verified against Password Issuance Control System (PICS) records annually.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The legal authority to collect this information is derived from the Immigration and Nationality Act, 8 U.S.C. §§ 1101, 1103, 1304 et seq., and 1360 and the implementing regulations found in 8 CFR.

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

Privacy Risk: Collection of non-essential information.

Mitigation: CIS and other systems that interface with NFTS collect additional data from applicants, but none of this information is maintained in NFTS. Only that information that is necessary to verify the file location. By limiting the user's view to A-number, location and status (e.g. request pending, charge out) contained in NFTS, USCIS limits the privacy impact as much as possible.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The Tri-Bureau uses the immigration file number to track active files throughout the three agencies and retrieve the file in support of adjudicating benefits, verifying documents, and enforcing immigrations laws.

Department of State (DOS) National Verification Center (NVC) performs inquiries in NFTS to determine the location of an immigration file in order to forward documents for interfiling.

USCIS uses the A-Number to request retired files back from NARA Federal Record Center (FRC); the FRC uses the following information from NFTS to retrieve the file: A-Number, requesting office address, NARA retirement accession number and NARA box number.

2.2 What types of tools are used to analyze data and what type of data may be produced?

NFTS does not analyze data for the purpose of identifying previously unknown areas of concern.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

NFTS does not make use of commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Privacy Risk: Unauthorized access to information.

Mitigation: Access to NFTS is given only to users that need it to perform their work. In addition, all users must be authenticated by user IDs and passwords. User privileges are governed by role assignments (i.e., non-records user, records user, and administrator). The Tri-Bureau have established standard operating procedures that stipulate proscribed and permitted activities and uses, auditing requirements, and integrity controls.

Privacy Risk: Outdated or inaccurate information.

Mitigation: The quality of the PII used by the system can be a risk, since it is extracted data from other noted systems. However, USCIS has procedures in place to check the data accuracy of information coming into NFTS, including semi-annual audits of all FCO files. Authorized USCIS Records personnel have the ability to correct inaccuracies brought to their attention internally, as well as by members of the public (via an amendment request).

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

The data contained in NFTS is destroyed or deleted when no longer needed for agency business per the NARA-approved disposition schedule [N1-566-06]. USCIS controls the subject's A-File for 100 years from the date of birth, and then transfers the files to NARA for permanent retention. NFTS continues to store the file location information even after a file is retired for accurate records keeping purposes.

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

NARA approved the NFTS retention schedule [N1-566-06-1] on March 9, 2006.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Privacy Risk: Retention of data for longer than necessary.

Mitigation: All data is retained for the indicated periods to fulfill the business requirements of DHS, which includes adjudication of immigration decisions, law enforcement uses, protection of national security, responding to requests within DHS, as well as those requests from other government agencies requiring historical and/or biographical information on the individuals of interest. A-File information has been determined to be of historical value and therefore NFTS information must be maintained for those purposes.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

NFTS generates reports containing A-Number and file location to facilitate the identifying of files to be reviewed, corrected, or entered into the Reengineered Naturalization Application Casework System[4] (RNACS). NFTS sends Refugee, Asylum, and Parole System (RAPS)[5] the A-Number and date of transaction and generates report outputs. NFTS obtains the receipt number and some fields are shared for generating report outputs with CLAIMS 3 and CLAIMS 4.[6] NFTS interfaces with Electronic Document Management

[4] Please see the Reengineered Naturalization Casework System PIA at: www.dhs.gov/privacy.
[5] Please see the Refugees, Asylum, and Parole System and the Asylum Pre-Screening System PIA at: www.dhs.gov/privacy.
[6] Please see the USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum PIA for CLAIMS 3 and the Computer-Linked Application Information Management System PIA for CLAIMS 4 at: www.dhs.gov/privacy.

System (EDMS) to obtain the location of electronic records.[7] NFTS generates a data file (A-number, requesting office, accession number, and box number) which is sent to the FRC to request retired files.[8]

NFTS shares the general location of the file with USCIS systems: CIS, RNACS, RAPS, CLAIMS 3, CLAIMS 4, and EDMS. CBP and ICE have direct access to NFTS for the purpose of tracking immigration files throughout the Tri-Bureau.

4.2 How is the information transmitted or disclosed?

ICE and CBP have direct access to NFTS.

To provide the physical location of an A-File, NFTS electronically interfaces, receives, and transmits data with the following USCIS systems:

CIS - USCIS stores active and retired immigrant information in this system. It includes tracking information on which FCOs maintain immigrant files. NFTS processes file movement transactions within an office. Each transaction processing a file movement into or out of an office or FRC is reported to CIS through the NFTS/CIS interface. There are several transaction types: transfer in, transfer out, transfer forward, file retirement, file accession change, and FRC return.

CIS provides the names of the FCO that maintains the immigrant file, file location, and whether the file has been retired. The date of birth of the record subject is derived from CIS for the purpose of generating the "records pull" tickets that facilitate locating, pulling, and charging out or transferring requested immigration files.

RNACS – NFTS provides for an automated data exchange between the two systems to facilitate the identifying of files to be reviewed, corrected, or entered into RNACS. NFTS provides file location information and reporting capability.

RAPS – Information sent to RAPS includes the A-Number and the date of the transaction. Report outputs include the RAPS Interface Pick List, Potential Enforcement EARM/NAILS Hit, Administrative No Show List, Decision Pickup Schedule List and Decision Pickup No Show List reports.

CLAIMS 3 or **CLAIMS 4** – NFTS obtains the receipt number from these systems, and some fields are shared for generating report outputs. Report outputs include the Record Summary and the Transactions Completed reports.

EDMS – USCIS scans the contents of an immigrant file and electronically stores the digital images in this system. EDMS sends updates to NFTS on a daily basis with the location of the digitized file, which allows NFTS to notify the system user that the immigration file is electronically available in EDMS.

---

[7] Please see the Integrated Digitization Document Management Program PIA at: www.dhs.gov/privacy.
[8] Please see the NARS-5/Center Information Processing System (CIPS)/Space Information System (SIS) PIA at: http://www.archives.gov/foia/privacy-program/privacy-impact-assessments/nars-5-pia.pdf.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risk: Unauthorized use of information by internal sharing partners.

Mitigation: Information in this system is safeguarded in accordance with applicable laws, rules and policies. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards that include restricting access to authorized personnel who have a need-to-know. All internal components are mandated by DHS to take mandatory Sensitive System Security training each year and to comply with DHS' Sensitive System Security guidelines. Tri-Bureau's users are trained on how to interpret and use immigration information.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

USCIS shares NFTS information with DOS NVS and NARA FCR.

USCIS provides DOS NVS with a read only view of NFTS. Access to this system allows DOS NVS to identify the location of an A-File. The DOS NVC uses this information to forward documents to the A-File location for interfiling.

USCIS requests the file location of retired files from NARA FRC. NFTS interfaces with CIPS to request retired immigration files. CIPS is NARA's system used to keep track of accession and locations of retired files. NFTS provides the following information to FRC to retrieve the file form storage: A-Number, requesting office address, retirement accession number and box number.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

A Memorandum of Understanding (MOU) exists between DHS and DOS that fully covers the information sharing. The MOU clarifies the authority for DOS and DHS to share immigration-related records and the basic mechanisms established to protect this data. Furthermore, the sharing of information is compatible with the routine uses outlined in the DHS/USCIS-001 Alien File (A-File) and Central Index System (CIS) SORN last published on January 16, 2007 (72 FR 1755).

USCIS retires the inactive A-Files to NARA/FRC. The immigration file number, accession number, and box number for file requests are extracted from NFTS and electronically transmitted via CIPS to NARA FRC, which initiates the process for pulling and returning inactive files to USCIS.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

USCIS provides DOS NVC employees with limited, read-only access to NFTS. The information in NFTS is -controlled and access is granted only to individuals (internally and externally) with a specific need to access the system in order to perform their duties. Each DOS NVS system user is provided a DHS-issued User ID and unique password to access NFTS.

USCIS electronically requests the return of retired immigration file from NARA via the NFTS-CIPS interface. NARA uses strictly defined data fields, which enables error checking and validation of the transmitted information. Personal data is limited to the A-Number and the User ID for the person responsible for requesting retired files. Additionally, any information shared with organizations outside the Department is required to be appropriately secured per Office of Management and Budget Memorandums 06-15, *Safeguarding Personally Identifiable Information*, and 06-16, *Protection of Sensitive Agency Information*.

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

Privacy Risk: Unauthorized access to, or disclosure of, information contained with NFTS.

Mitigation: To mitigate this risk, Records Division personnel strictly control the process of data sharing. Only the minimum necessary information is sent over this interface. An updated NFTS Interconnection Security Agreement with NARA will be put in place as soon as possible. DOS NSV has "view only" access and cannot manipulate any data within the system. They also do not receive pull tickets

or file requests and therefore do not see any names or dates of birth associated with an A-Number.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

NFTS is not the original point of collection and extracts data from systems identified in section 1.2. Individuals are provided general notice through the DHS/USCIS-001 Alien File (A-File) and Central Index System (CIS) SORN (72 FR 1755) and this PIA.

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

Applicants who seek USCIS benefits are presented with a Privacy Act Notice and a signature release authorization on the relevant benefit application/petition. The Privacy Act Notice details the authority and uses of information. The form is signed by the applicant indicating that s/he certifies and authorizes the release of any information from the applicant's record that USCIS needs to determine eligibility. Applicants are told at the point of data collection (generally in the form itself) that it is within their rights to decline to provide the required information; however, it will result in the denial of the applicant's benefit request.

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

The extent of notice and opportunity to provide informed consent vary based on the particular purpose associated with the original collection of the information in the systems of records from where the information is extracted. In most cases, notice is provided when the applicant fills out the form or application for benefits. In the law enforcement or national security contexts, notice or opportunity to consent would compromise the ability of the agencies to perform their mission. In cases such as these, notice and consent may not be available. All PII in NFTS is extracted data from other systems as noted above. Although individuals do not have a right to consent to particular uses, USCIS tailors the amount of PII used by NFTS to what is needed in a particular file tracking activity so that only the minimum PII necessary to perform the function is used.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Privacy Risk: Individuals are not provided direct notice of their information in NFTS.

Mitigation: USCIS provides the individual notice through the benefit application and this PIA. The USCIS application contains a provision by which an applicant authorizes USCIS to release any

information from the application as needed to determine eligibility for benefits. Individuals applying for USCIS benefits are made aware that the information they are providing is being collected to determine whether they are eligible for their respective benefit. The immigration file is necessary for the benefits adjudication process. USCIS uses NFTS to expedite the search and retrieval of the subject's immigration file within the Tri-Bureau.

For immigration files used for other purposes (e.g., enforcement, investigations), the individual is not provided notice.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

To obtain access to their information, the individual would have to make either a Freedom of Information Act or Privacy Act request. Individuals who are seeking information pertaining to them are directed to clearly mark the envelope and letter "Privacy Act Request." Within the text of the request, the subject of the record must provide his/her full name, date and place of birth, and notarized signature, and any other information which may assist in identifying and locating the record, and a return address. For convenience, individuals may obtain Form G-639, FOIA/PA Request, from the nearest DHS office, to submit a request for access. The procedures for making a request for access to one's records can be found on the USCIS website, located at www.uscis.gov.

An individual that would like to file a FOIA/PA request to review their USCIS record may do so by sending the request to the following address:

U.S. Citizenship and Immigration Services
National Records Center
FOIA/PA Office
P O Box 648010
Lee's Summit, MO 64064-8010

7.2 What are the procedures for correcting inaccurate or erroneous information?

Information in NFTS is extracted data from other systems as noted in Section 6.1. Individuals may direct all requests to contest or amend information to the FOIA/PA Office at USCIS. They must state clearly and concisely in the redress request the information being contested, the reason for contesting it, and the proposed amendment thereof. Clearly mark the envelope "Privacy Act Amendment."

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 application instructions, DHS/USCIS-001 A-File and CIS SORN (72 FR 1755), the USCIS website, through this PIA, and by USCIS personnel who interact with them.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Individuals are provided opportunity for redress as discussed above.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Privacy Risk: Incorrect information pertaining to individuals.

Mitigation: NFTS contains information pertaining to the location of a file. Subject information is limited to the primary tracking number, name, and date of birth, which is extracted from other USCIS systems noted in Section 6.1. Access to data in NFTS is limited to those with a need-to-know. The extracted data from other USCIS systems have access and correction procedures noted in their respective system notices.

Privacy Risk: Agency may be unable to locate a file due to inaccurate location information in NFTS.

Mitigation: When the file location is not the same location displayed in NFTS, the USCIS Records Division personnel conducts a manual search request of microfilm records at Headquarters if one of the following applies:

- The person has an A-Number under 12 million or between 30 and 35 million.
- The A-File was created prior to December 31, 1975.
- Non-immigrant records prior to January 1938.
- Naturalization or Citizenship records dating between 1906 and April 1, 1956.

USCIS sends the request for a manual search internally to a specified records mailbox. A separate request is required for each subject. Manual search/historical files request processing time varies with workload. If the historical file requested is in the FRC, additional time is required for FRC processing and shipment of the file.

If the file does not fall into one of the above categories, the last office known to have the file conducts a special search and any subsequent offices until the physical file is found.

Section 8.0 Technical Access and Security

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

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

Each NFTS user must submit a completed G-872B to the local PICS office to gain access to NFTS. Once approved, the local PICS office grants access to the NFTS system, then grants the users access to transactions needed to perform their duties. In addition, the local NFTS administrator assigns a role that governs the user's access right. Access to NFTS is controlled via the DHS PICS office, which controls user authorizations and authentication controls for all DHS system users. The PICS office has documented procedures for verifying user authorization and suitability before granting access. NFTS follows access procedures documented in NIST 800-53, the DHS Sensitive System Handbook and the NFTS System Security Plan.

NFTS users sign DHS Rules of Behavior (ROB) which detail how users are to operate the system. The DHS ROB is given to users when they complete the mandatory security application for access to NFTS. Users acknowledge they have read, understand, and agree to the content of these rules. These rules cover system access, passwords and other access control measures, data protection, use of government office equipment, software, Internet and e-mail use, incident reporting, and accountability. They acknowledge, by signing and dating the DHS ROB that violating the system rules of behavior will involve potential disciplinary actions. The DHS PICS office maintains copies of these rules. The local PICS office keeps the original ROB signed by the user, and the user is given a copy. The PICS Office also ensures all contractors and new system users sign ROB.

NFTS ensures that each user is authenticated before accessing the NFTS system. Each user of the system is uniquely identified. Users are authenticated each time they log on to the system.

8.2 Will Department contractors have access to the system?

Contractor personnel have access to NFTS and perform maintenance software support to correct system problems, maintain the servers and databases, and provide the hosting facility and network where NFTS resides.

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

All NFTS users complete annual mandatory Privacy and Security Awareness training. This training includes guidance on federal laws, policies, and regulations relating to privacy and data integrity, as well as the handling of Sensitive but Unclassified/For Official Use Only Information. The USCIS OIT IT Security office verifies that training has been successfully completed and maintains a record of certificates of training on all USCIS employees and contractors.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

NFTS was granted a Certification and Accreditation (C&A) on April 22, 2008. The C&A is valid for

three years from this date.

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

Users are authenticated before access is permitted. Each user must be approved to access NFTS prior to accessing the system, and assigned a role appropriate to his or her job responsibility. NFTS servers capture significant audit and history information on all NFTS transactions that is sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. These records include all metadata changes, alien file deletes, last successful login and all user actions within NFTS.

NFTS system administrators are frequently logged on to the NFTS servers and are the first line of defense. The system administrator regularly looks at the server audit events during the course of their daily duties for unusual activities and actions that are not normally present in the logs. The system administrators are thus the most likely to see that something is wrong from looking at the event logs. The event log data is provided to the Information System Security Officer for review on a monthly basis. The event log data does not contain any PII.

Upon detection of any suspicious activity, the DHS Computer Security Incident Response Center is notified.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Primary Risk: Unauthorized access to or disclosure of information contained within NFTS.

Mitigation: This risk is mitigated through various safeguards, such as access controls and the use of technology safeguard such as intrusion detection systems. Access to NFTS is restricted to the level needed for users to perform their duties. NFTS is maintained in a secure hosting facility. Physical controls of the facility including guards and biometric access prevent entry by unauthorized personnel.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

NFTS was custom built to provide a website on the DHS Intranet to replace its predecessor, the Receipt and Alien-File Accountability and Control System and NFTS version 2, a client/server-based application.

9.2 What stage of development is the system in and what project development life cycle was used?

NFTS is in the operations and maintenance phase of the DHS System Development Life Cycle Methodology.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

NFTS is used to track and log the movement of immigration files throughout the Tri-Bureau. NFTS does not employ technology which may raise privacy concerns.

Responsible Officials

Donald K. Hawkins
Privacy Officer
US Citizenship and Immigration Services

Approval Signature

Original signed copy on file with the DHS Privacy Office
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security