Privacy Impact Assessment
for the

Fraud Tracking System (FTS)

June 24, 2005

Contact Point
Tarrazzia Martin
Office of the Chief Information Officer
U.S. Citizenship and Immigration Services
(202) 272-1700

Reviewing Official
Nuala O'Connor Kelly
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

SUMMARY:

System Name:	System Name: Fraud Tracking System (FTS)
SORN that this System Operates Under	Computer Linked Application Information Management System (CLAIMS 3 and 4) Justice/INS-013 October 4, 2002 Published in the Federal Register Volume 67, Number 201, October 17, 2002 on pages 64132-64134
System type and connectivity	The system is identified as a Major Application (MA) in the DHS Systems Inventory and is considered a networked system. FTS is considered "Sensitive" because it receives, stores, and processes Personal Identifiable Information (PII).

1. Introduction

Protecting the personal information of employees and citizens is a key part of the mission of the Department of Homeland Security (DHS) and the U.S. Citizenship and Immigration Services (USCIS). As USCIS increasingly relies on information systems to meet its mission, the importance of protecting information, particularly personal information, also increases. In order to meet the challenge of sharing and collecting information, a privacy impact assessment (PIA) has been performed to identify how the personal information is being used in USCIS' new Fraud Tracking System (FTS), and what safeguards are implemented to ensure the appropriate protections. This PIA helped system owners identify whether information practices meet the requirements of privacy and security laws.

1.1. The Office of Fraud Detection and National Security (FDNS)

The Office of Fraud Detection and National Security (FDNS) within USCIS was created to enhance the integrity of this Country's legal immigration system by detecting, deterring, and pursuing immigration benefit fraud, and identifying persons seeking benefits who pose a threat to national security and/or public safety. FDNS plays a pivotal role in enabling USCIS to accomplish its mission of providing the right benefit to the right person at the right time, and no benefit to the wrong person. It does this by:

- Detecting and combating immigration benefit fraud;
- Conducting and overseeing law enforcement (background) checks on persons seeking immigration benefits;

- Performing as USCIS' primary conduit to/from the law enforcement and intelligence communities; and,
- Identifying vulnerabilities and other weaknesses that compromise the integrity of the legal immigration system.

FDNS was created at the inception of USCIS in 2003 as the foundation of its anti-fraud strategy. GAO Report 2-66 concluded that this Country's legal immigration system was being used to further illegal activities and/or activities that threaten national security and public safety. GAO also concluded that the legacy INS did not have an anti-benefit fraud strategy; did not designate it as a priority initiative; and did not have a mechanism to collect and report data aimed at identifying the volume and type of benefit fraud that exists.

The FDNS has, in a very short time, created a program that addresses both fraud prevention and nation security/public safety in a systematic integrated way.

1.2. The Fraud Tracking System (FTS)

In support of the important role of decreasing fraud in the immigration system, FDNS has developed the Fraud Tracking System (FTS). FTS is a case management system used to track and control immigration fraud inquiries and investigative referrals, which includes tracking interaction with Immigration and Customs Enforcement (ICE) in cases that may involve law enforcement activities. FTS allows users to conduct queries of Computer-Linked Application Information Management System (CLAIMS 3) immigrant benefit data to identify potentially fraudulent applications for immigration benefits (CLAIMS 3 is the main system used by USCIS to administer benefits to immigrants).

An inquiry may be generated in two ways:

1. Queries against the CLAIMS 3 database that identify potential actions that are not consistent with a certain type of benefit being applied for (e.g., a person sponsoring multiple fiancés at the same time or a religious worker application filed by a religious organization with an address that is actually a Post Office box).
2. External leads such as tip letters or phone calls, news articles, and interviews by USCIS officers during the course of a benefits application

When an FDNS Officer identifies suspicious activities either from a tip or searching the CLAIMS 3 data base, a lead will be opened in FTS and an FTS Identifier will be created. The FTS Identifier is a unique system-generated number that is not specifically tied to an individual. This number is not recorded in the CLAIMS 3 system.

The inquiry may include investigative reports, administrative inquiry reports, or biographical information on an individual or a group of individuals. It is only after the completion of the inquiry that a note will be made in CLAIMS 3 as to the results of the inquiry.

This new program is an automated implementation of an existing manual paper-based process. FTS is a multi-phased project and is currently in its first phase. As future phases are developed, this PIA and applicable System of Records Notice (SORN) will be updated.

2. Data and Its Purposes

2.1. Description of Information Collected – Nature and Source

FTS creates a unique identifier at the time an inquiry is initiated. The FTS Identifier is a unique system-generated number that may or may not be specifically tied to an individual. This number is not recorded in the CLAIMS 3 system.

An FDNS officer will, upon the initiation of an inquiry, pull additional data from the CLAIMS 3 system. This additional data can include the following:

- Subject Name(s)
- Subject Social Security Number (SSN)
- Subject Date of Birth (DOB)
- Subject Country of Birth (COB)
- Subject Maiden Name
- Subject Address
- Taxpayer ID
- Telephone Number
- Alias Name(s)
- Alien Registration Number (A-Number)

In addition to this information, the FTS may also contain information from law enforcement agencies, public institutions, interviews of witnesses, public records, observations, sworn statements, official reports and members of the general public based upon the results of the inquiry. All of this information presently is maintained in either CLAIMS 3 or as part of the paper inquiry file attached to the Alien-File (A-File, the immigration status file). This additional information is entered and stored in CLAIMS 3.

Records are indexed and retrievable by name or Alien File number or Receipt File number.

In addition to the personal information collected as part of an inquiry, the FTS system will allow FDNS Officers to save the queries used to identify possible fraud. The query structure and rules can be saved within FTS, but not the actual query results.

2.2. Why the Information is Collected

This information is being retrieved from the USCIS owned and operated CLAIMS 3 system in order to process immigration fraud inquiries and investigative referrals. The information contained in FTS is relevant and necessary to fraud investigations conducted by USCIS.

2.3. Intended Use of the Information

FTS is a case management system used to track and control immigration fraud inquiries and investigative referrals. FTS users conduct queries of CLAIMS 3 data to identify potentially fraudulent applications for immigration benefits. In many instances, this requires FTS users to look for patterns within large numbers of applications at different times. This practice may require users to save those queries/searches/rules to be run periodically against updated lists of applications to see if new patterns arise that indicate fraud is occurring or if new applications have been filed that fit those same fraud patterns.

2.4. Information Sources and Acquisition

CLAIMS 3 receives its data directly from individuals seeking benefits from USCIS. All data stored or otherwise utilized by FTS is provided through the CLAIMS 3 system. Individuals who file USCIS applications and reports supply the basic information contained in this system. Other information comes from law enforcement agencies, public institutions, interviews of witnesses, public records, observations, sworn statements, official reports and members of the general public. This additional information is entered and stored in CLAIMS 3.

The FTS system does not collect data directly from individuals.

2.5. Data Sharing with Other Organizations and Its Intended Use

During Phase 1, the system will not share data with any other organizations. If and when this sharing needs to occur, this PIA and associated SORN will be updated, published, reviewed, and approved before any information sharing occurs.

2.6. Consent and Declining to Provide Information

The information used by the FTS system is collected under the CLAIMS SORN, which includes CLAIMS 3 and CLAIMS 4. Through the application process, individuals have consented to the use of the information for fraud detection purposes.

2.7. How the Information is Checked for Accuracy

Before disseminating any records about an individual to any person other than an a Federal Agency, unless the dissemination is made under the Freedom of Information Act (FOIA), USCIS will make reasonable efforts to ensure that such records are accurate, complete, timely, and relevant on each system for agency purposes.

The information is checked for accuracy by the CLAIMS 3 system. This is done through database technical controls, inherent business logic built into the system, and a manual review process (e.g., interviews with the individuals). Improved processes are being put in place for periodic review of PII contained in the system to ensure it is timely, accurate, and relevant. A notification process is also being put in place so that when changes occur (i.e., revisions to PII or when the CLAIMS 3 system encounters a major change or is replaced) other resources dependent upon PII contained in this system are alerted.

2.8. Information Requests

Requests for access to a record from this system must be in writing. If a request for access is made by mail the envelope and letter shall be clearly marked "Privacy Act Request." The requester will include a description of the general subject matter and if known, the related A-File or Receipt File number and any other identifying information which may be of assistance in locating the record. To identify a record relating to an individual, the requester should provide his or her full name, date and place of birth, verification of identity (in accordance with 8 CFR 103.2(b)), or a statement acknowledging penalty of perjury, and any other identifying information which may be of assistance in locating the record. The requester shall also provide a return address for transmitting the records to be released. Requests for information should be made to USCIS FOIA/PA Officer at 111 Massachusetts Avenue NW, Washington DC 20001.

2.9. Access to and Correcting Erroneous Information

Any individual desiring to contest or amend information maintained in CLAIMS 3 and thus FTS should direct his or her request to the USCIS FOIA/PA Officer at 111 Massachusetts Avenue NW, Washington DC 20001. The request should state clearly what information is being contested, the reasons for contesting it, and the proposed amendment to the information.

If USCIS intends to use information that is not contained in an applicant or petitioner's application or supporting documentation, it will provide formal notice to said entities and provide them an opportunity to refute the information prior to rendering a final decision on his or her application/petition. This provides yet another mechanism for erroneous information to be corrected. This is required by case law; it is not discretionary.

2.10. Retention and Destruction

The CLAIMS SORN governs the retention of personal information collected by FTS as described below.

Information in FTS will be archived in accordance with the CLAIMS 3 LAN data base retention schedule. Archiving criteria for each different USCIS form downloaded into the system is generally as follows: one to three years after date of last completed action to a repository where it will remain 15 years before destruction. Archived reports are maintained at USCIS Service Centers for 15 years and are then destroyed. The reengineered client/server data will be deleted 15 years after USCIS has completed the final action on the benefit request.

The Retention and Destruction requirements and policies are currently under review by USCIS Management. Any proposed changes will be updated in applicable SORNs and PIAs, as required.

3. Policy, Procedures, and Other Safeguards

3.1. Training

USCIS trains each of its Immigration Officers and Intelligence Research Specialists extensively and continuously on the proper use of information and each of its analysis and query tools. This training is updated and reinforced each time a new tool such as the pattern analysis module of FTS is introduced. This proactive training approach also helps address potential concerns that these tools could be used inappropriately. In addition, our FTS functional administrators provide oversight and auditing of the types of queries being conducted. These reviews are done on a regular basis.

In compliance with Federal Information Security Management Act, OMB Policy, NIST guidance, and DHS/USCIS Policy requirements, all users and administrators of the systems associated with the FTS have been appropriately trained in the past year on the Rules of Behavior and consequences for violating the rules. The Rules of Behavior must be read, acknowledged, and signed by FTS users in order for them to use the system.

USCIS has implemented security awareness training as an annual refresher training requirement for users of all USCIS standard workstations. All users are required to complete computer security awareness training before they are permitted access to unclassified USCIS networks and email. This initial security awareness training must be completed prior to requesting access to the FTS. All users will be required to sign (and verified by their supervisor's signature) that the access they are requesting is within the scope of their official responsibilities. The prohibitions and possible punishments for misuse are clearly outlined on the user access form. Online and interactive security training and awareness are given to all Government and contractor support staff associated with the FTS as well.

Given the sensitivity of the information and the use of the system, it has been determined that FDNS officers must hold a higher security clearance than other staff in the USCIS District Offices, National Benefits Center and Service Centers. With this higher level of clearance, individuals are given additional training on the sensitivity of the information and the need to use the information appropriately. Furthermore, FDNS has in place procedural safeguards including adverse personnel actions for misuse or misappropriation of data.

3.2. Management, Operational, and Technical Safeguards

Access to FTS Phase I will be limited to FDNS staff, system administrators, and developers. The FTS system uses role based access controls outlined in the FTS User manual and System Security Plans. The current process for providing user access to FTS is granted only by the System Owner. Technical Security controls for the database, operating system, application, and network have been deployed as well. The criteria, procedures, controls, and responsibilities regarding access are documented in the FTS System Security Plan prepared as part of the NIST SP 800-37 Certification and Accreditation (C&A) activities.

A basic audit trail is available in FTS and is routinely reviewed.

3.3. Physical Safeguards

USCIS has also enacted physical security measures that encompass the full range of protective measures designed to prevent unauthorized access to, and the loss, theft, destruction, sabotage, or compromise of equipment, facilities, material, and information. Physical controls include barriers, badges, guard or security forces, supporting infrastructure, contingency and emergency support, facility intrusion detection systems, and surveillance systems.

Users access FTS via the DHS Intranet from USCIS Service Centers, the National Benefits Center, and Field Offices. These facilities are resident in DHS owned or leased facilities. The DHS Intranet is a private wide area network. The system is not accessible from the Internet nor does the public have access to the system or its data. Allowable access and disclosure of this information is described in the CLAIMS SORN.

4. Maintenance of Administrative Controls

The USCIS OCIO IT Security Office has developed and follows a security program that is compliant with the Federal Information Security Management Act (FISMA). The FTS system is currently undergoing the Certification and Accreditation (C&A) in compliance with FISMA. An Interim Authority to Operate (IATO) will be granted upon acceptance of this PIA.

5. Summary and Conclusions

As an organization, both USCIS and the FDNS are committed to the safeguarding of personally identifiable information (PII). The Fraud Tracking System (FTS) 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.

Changes were not made to system architectures, hardware, software, or implementation plans as a result of this PIA. However, this PIA has resulted in some further refinement of the Systems Security Plan (SSP) and justification for detailed auditing in subsequent releases of the system. Leveraging this PIA and associated SORN, we will develop mitigation strategies and a Plan of Action and Milestones for Risks identified as a result of the NIST SP 800-26 Self Assessment and NIST SP 800-37 Certification and Accreditation package.

FTS is a multi-phased project and is currently in its first phase. As future phases are developed, this PIA and applicable System of Records Notice (SORN) will be updated to address those updates.

6. Point of Contact Information

The USCIS POC is the following:

Tarrazzia Martin, CIO
U.S. Citizenship and Immigration Services
(202) 272-1700

USCIS and the Department welcome your comments on this FTS privacy impact assessment. Please write to: Privacy Office, Attn: FTS PIA, U.S. Department of Homeland Security, Washington, DC 20528, or email privacy@dhs.gov. Please include FTS PIA in the subject line of the email.