FPS FISTS
NPPD
DHS Privacy Office
Department of Homeland Security
Washington, DC
PIA@dhs.gov

PRIVACY IMPACT ASSESSMENT (PIA) 3-YEAR REVIEW COVER PAGE

Component: *NPPD*
Name of Program/System: *Federal Protective Service Information Support Tracking System (FISTS)*
This system has undergone a PIA 3-Year Review on: *October 4, 2012*

The DHS Privacy Office works with DHS components to ensure that PIA reviews are conducted every three years.

DHS requires each component PIA to be reviewed in conjunction with the expiration of the accompanying PTA, in an effort to determine whether significant changes have been made to the system. This review ensures that each system continues to accurately relate to its stated mission.

Specifically, the PIA 3-Year Review Adjudication addresses each of the main areas of the PIA relating to: Legal Authorities; Characterization of the Information; Uses of the Information; Notice; Data Retention; Information Sharing; Redress; and Auditing and Accountability.

The above mentioned PIA has had no changes to the privacy risks and mitigations identified in the published PIA.

Additionally the contact information listed on the PIA has changed. The new contact information is:

L. Eric Patterson
Director, Federal Protective Service
National Protection and Programs Directorate
(202) 732-8000

Privacy Impact Assessment
for the

Federal Protective Service Information Support Tracking System (FISTS) Contract Suitability Module

September 16, 2009

Contact Point
Gary Schenkel
Director, Federal Protective Service
U.S. Immigration and Customs Enforcement
(202) 732-8000

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

Abstract

The Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) Federal Protective Service (FPS) Information Support Tracking System (FISTS) Contract Suitability Module is a web-based application used to automate the process for assessing the suitability of FPS and General Services Administration (GSA) contract personnel to work in secure Federal buildings, and to track periodic background re-investigations of those contract employees. The system collects and maintains information on applicants and contractor personnel who work in secure Federal buildings such as security officers, childcare workers, cleaners, and other contracted service positions. ICE is conducting this Privacy Impact Assessment (PIA) because FISTS collects and uses personally identifiable information (PII) on members of the public who seek or are currently employed in these positions within Federal facilities.

Overview

The FPS Information Support Tracking System (FISTS) is a web-based system used to input, manage, and track information regarding the suitability of contracted service personnel within secure Federal facilities, contract guard certifications, and physical security in Federal facilities. FISTS is owned and operated by ICE's Federal Protective Service (FPS) within the Department of Homeland Security (DHS). The FPS mission is to render Federal properties safe and secure for Federal employees, officials, and visitors in a professional and cost effective manner by deploying a highly trained and multi-disciplined police force. FPS provides alarm monitoring and uniformed police response as well as investigative resources pertaining to incidents and offenses that take place in and around Federal buildings. FPS also adjudicates the suitability of FPS and GSA contracted service personnel to work in Federal facilities.

The FISTS application consists of four modules, only one of which collects and maintains PII about members of the public. That module is called the Contract Suitability Module (CSM) and is discussed in this PIA. CSM is a web-based application used to automate the process for assessing the suitability of personnel to work in secure Federal buildings. It also supports the periodic background re-investigations of these contract personnel. CSM collects information on individuals who have or seek employment in certain job categories through a contractor in Federal buildings secured by FPS, specifically, contract FPS security officers. It also collects information on GSA contract personnel or applicants such as childcare workers, cleaners, and other GSA contracted service personnel. These individuals are subject to a background investigation seeking to determine whether they are suitable for the position and for access to a Federal facility. Pursuant to an agreement with FPS, the Office of Personnel Management (OPM) conducts these background investigations and provides FPS with the results so FPS can make the final suitability determination. FPS uses CSM as the centralized database to enter, update, and track records of the individuals undergoing these background investigations and to record the final suitability determination made by FPS.

FPS collects information about these individuals through standard Federal background check forms completed by the individual and submitted to FPS by the contractor. The individual completes either Standard Form (SF) 85P or 86 depending on whether the job is considered a public trust position or

national security position, respectively. While these forms collect a significant amount of PII, only a limited subset of that information is entered into CSM because the system is only used to track and manage the background check process. CSM does not serve as the official repository for the background check investigative file and therefore does not capture all information related to the investigation itself. Fingerprints are also collected as part of the background investigation process, however, they are not collected, processed, or retained in the FISTS system or the CSM.

The other three FISTS modules are the Certification Employment Requirement Tracking System (CERTS), which manages FPS contract guard certifications such as CPR and firearms training; the Security Tracking System (STS), which manages Federal facility security countermeasure records for tracking and auditing purposes; and the Administration Module, which provides system administration functions for the other three modules in FISTS. While these other modules may contain PII about individuals, a PIA is not required because they do not contain information on members of the public. In addition, the modules do not contain PII of individuals from more than one component.[1] In December 2009, FPS anticipates transitioning the entire FISTS system to the DHS Integrated Security Management System (ISMS).[2]

Contract Process

A private company is awarded a government contract to provide security officers to secure certain Federal facilities protected by FPS. The company hires an individual to serve as a security officer under the contract and has that individual complete an SF-85P or SF-86 application package. The company submits the completed package to FPS. FPS creates a FISTS record through the CSM and enters certain identifying data about the individual (such as name, address, date of birth) from the SF-85P/86 into the record. FPS also enters information about the position for which the individual is being considered. Using a separate system owned by OPM known as Electronic Questionnaire for Investigation Processing (e-QIP), FPS electronically forwards the SF-85P/86 package to OPM and requests that OPM begin the background investigation. OPM then electronically sends status reports to CSM containing information on the progress of the case, such as "open" or "closed," and the date the OPM interview was scheduled and completed. This data is then uploaded into the appropriate data fields in CSM. Separately, FPS requests a fingerprint-based criminal records check from the FBI and manually updates CSM if a criminal history record on the individual is found to exist. When the investigation is completed, OPM submits the background investigation file in paper copy to FPS, which makes the final suitability determination and records it in CSM. FPS then advises the contractor whether the individual is suitable for employment in a secure Federal facility.

[1] Please see the Privacy Policy Guidance Memorandum, December 30, 2008 (2008-02) for additional information. http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf

[2] Please see the Personnel Security Activities Management System (PSAMS)/Integrated Security Management System (ISMS) Update Privacy Impact Assessment at www.dhs.gov/privacy for additional information.

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?

CSM collects information on individuals who have or seek employment in certain job categories through a contractor in Federal buildings secured by FPS, specifically, contract FPS security officers, and GSA contract personnel such as childcare workers, cleaners, painters, construction workers, and other GSA contracted service personnel. These job categories are maintained (created or modified) by CSM Administrators. CSM also includes information related to background re-investigations of contractor employees, which take place approximately every five years. CSM maintains the following categories of information on the system and on the backup tapes:

- Individual Identifying Data: full name, home address, Social Security Number (SSN), date of birth, sex, height, weight, eye color, hair color, marital status, race, citizenship, Alien File Number (A-Number).
- Case Record Data: job category, date of application, date OPM interview scheduled and held, OPM background investigation case status (open or closed), FPS suitability decision (possible values for this field are: preliminary favorable, preliminary unfavorable, final favorable, final unfavorable).
- FBI Criminal Record Check Response: The FBI response to the fingerprint-based criminal history record check contains the following data which is manually entered into CSM: criminal history record exists (possible values for this field are: Yes or No).

Because OPM performs the background investigation for FPS, it produces and retains the full investigative case file related to the background check, including a copy of the individual's SF-85P/86, and any other records collected, produced, and maintained by OPM investigators during the course of the investigation. Other than the data identified above, FPS does not enter any additional information into FISTS.

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

The contractor employee or applicant is the source of the Individual Identifying Data and provides that information to FPS by completing the SF-85P, Questionnaire for Public Trust Positions (OMB No. 3206-0191), or the SF-86, Questionnaire for National Security Positions (OMB No. 3206-0005) during the suitability clearance process. The forms are submitted to FPS through the contractor that employs or is seeking to hire the individual.

FPS personnel are the source of the Case Record Data, which details the job category and the date of the individual's application for the position. FPS personnel also input into CSM the suitability

determination made by FPS personnel based upon the findings of the OPM background investigators. (Other than what is described in Question 1.1 above, CSM does not contain any other information about the background check investigation itself; OPM retains that information separately.) OPM also provides some of the Case Record Data in CSM through electronic daily updates of the status of the background investigation through an interface with the OPM Personnel Investigation Processing System (OPM-PIPS). OPM-PIPS sends the following data to CSM: name and SSN (to identify the individual), case status (open or closed), and date OPM interview was scheduled and completed.

CSM also records whether there is a criminal record (yes/no) of the individual based upon the Criminal Record Check Response from the FBI's Integrated Automated Fingerprint Identification System (IAFIS), which is a national fingerprint and criminal history system that provides agencies with fingerprint-based criminal history information.

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

This information is collected to allow FPS to track and manage suitability investigations of individuals that have applied for or are incumbents in certain contract positions in Federal buildings that are protected by FPS. CSM provides for the automation of what would otherwise be a manual process.

PII is collected to adequately identify the individual in CSM so that additional information can be input into the appropriate record. The Case Record Data records information about which job category the individual is being considered for or is currently employed in, the status of the background investigation, and the FPS suitability decision. The Criminal History Record Check Response reflects whether there is a criminal history record for the individual on file at the FBI. CSM stores this information because the existence of a criminal history record will require further investigation and therefore additional time until it is completed. All of this information is collected and used to support the tracking and management purposes of CSM.

FPS makes suitability determinations for FPS security officer applicants and employees because these individuals work under contracts awarded by FPS, which needs to retain suitable individuals to serve as guards at FPS-protected Federal facilities. FPS makes suitability determinations for GSA contract applicants and employees because FPS used to be part of GSA prior to the formation of DHS in 2003. FPS continues to perform this service for GSA based upon a Memorandum of Agreement between FPS and GSA.

Backup tapes of the FISTS data are retained off site for 7 years in case the FISTS system data is compromised, altered or destroyed.

1.4 How is the information collected?

The information is collected from contractor employees and applicants using the SF-85P, or the SF-86 for those needing access to classified information. Using these forms, the contractor collects the information directly from its employees and then forwards it to FPS.

1.5 How will the information be checked for accuracy?

The accuracy of the individual's information is confirmed through several different means during the process, including physical verification of at least two forms of identity documentation, the results of fingerprint-based checks, and the OPM investigation which seeks to confirm information supplied by the individual on the SF-85P/86. Individuals may be asked to resolve or explain discrepancies and be given an opportunity to correct the information through an appeal process if an adverse suitability determination is made.

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

The authorities for the collection of information on Federal employees and contractor employees, and applicants for such positions, is found at 5 U.S.C. §§ 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 3309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397.

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

In any system that contains personal data, there is a risk of over collection of sensitive PII. In the case of CSM, this risk is mitigated by the limited amount of PII that is captured and entered into CSM. The individual's application package (SF-85P/86) contains a significant amount of highly sensitive personal data, including information about criminal convictions, mental health treatment, previous employment, and drug use; however, CSM only captures a subset of purely identifying data from the package including name, date of birth, and SSN. This narrowly focused collection of information is consistent with the limited purpose of the system – to track background investigations until they are concluded and a suitability determination is made. Since CSM is not the case management system for the background investigations, no additional information is required.

An additional issue posed by capturing key identifiers such as date of birth and SSN is the risk of unauthorized access to or disclosure of information that could put the individual at risk for identity theft. This is mitigated by training, the maintenance of secure passwords, and the practice of operational and informational security. Individuals who are found to have accessed or used CSM in an unauthorized manner will be disciplined in accordance with ICE policy.

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.

CSM contains limited PII about contract employees and applicants for contract positions, including the existence of criminal history records, and both favorable and unfavorable suitability determinations to ensure that they do not pose a security threat to Federal buildings and are suitable for employment as a contractor in a Federal facility. The information is used solely to support the tracking and management of these contract employees and applicants as they are investigated and as suitability determinations are made.

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

Several standard management reports are programmed into the system; through the use of filters specific reports can be generated on the data available, such as the 5 day average timeline report which tracks the time from entering the suitability process to the preliminary suitability determination The reports are available for view or print only.

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

The system does not use or maintain commercial or publicly available data. OPM may use commercial or publically available data during the course of their background investigations; however, no such data is entered into CSM.

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.

Only authorized government employees and contractors can access FISTS. All users of the FISTS system are required to take an annual Information Security Awareness course which includes privacy training. In addition, FISTS users are required to sign the DHS Rules of Behavior, which govern the actions of individual system users that utilize government IT systems within the agency. The minimum security controls in place are documented in the Certification and Accreditation documents that describe the implementation of managerial, operational, and technical security controls that comply with all applicable Federal laws, regulations, policies, guidelines, and standards.

FISTS workstations, servers and other computing equipment are contained in areas that have physical access controls including armed security guards with identification checks, locks and key card access. Physical access to the FPS Data Center where the FISTS servers are stored is controlled by a badge reader. Federal security officers screen access at the doorway and patrol throughout the facility. Access is layered with access permitted only to personnel authorized to maintain the FISTS system.

Section 3.0 Retention

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

3.1 What information is retained?

ICE retains all of CSM data described in Question 1.1. Backup tapes of the system are also retained. Recovery Manager (RMAN) software is used to backup FISTS database. A full backup is performed bi-weekly and an incremental backup is performed daily. A full backup of the Unix operating system is performed daily.

3.2 How long is information retained?

Pursuant to General Record Schedule 18, Item 22, the CSM records will be destroyed upon notification of individual's death or no later than five (5) years after separation or transfer of individual or no later than five (5) years after contract relationship expires, whichever is applicable. FISTS backup tapes are retained off site in a secure facility for seven (7) years.

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

ICE relies upon NARA's General Records Schedule 18, Item 22, for disposition authority for CSM records.

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

The privacy risk of data retention is that the information could be compromised, altered, lost or destroyed or unauthorized users could gain access. The five-year retention period after termination of the employee or contract is consistent with retention of background security files insofar as the information is no longer needed after the contractor is no longer working for the government. However, if the employee returns to working for the government or for another agency, the data will still be available for the five-year period. Thus, the retention period ensures that the information is available while the contractor is employed by the government, and a reasonable period thereafter, in case they should return to government work with this or another agency. The limited retention period will also minimize the privacy risks associated with maintaining this data, as does the limited amount of sensitive PII in the system.

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?

Information in FISTS is not shared with other DHS components.

4.2 How is the information transmitted or disclosed?

Information in FISTS is not shared with other DHS components.

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.

Information in FISTS is not shared with other DHS components.

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?

Information collected from the individual is shared with the following government organizations: the SF-85P/86 is shared with OPM for the purpose of conducting the background investigation, and fingerprints are shared with FBI for the purpose of conducting a criminal records check. FPS also shares the individual's suitability determination with the company that employs the individual (the contractor) and, where it pertains to a GSA contract, with GSA.

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.

Yes. Limited information may be disclosed outside of DHS to support the processing of background investigations and to convey the results of suitability determinations to the agencies and employers that need to know. SORN coverage for CSM data is provided by the Department of Homeland Security Personnel Security Management[3] (DHS/ALL-023, Jan. 16, 2009, 74 FR 3084), which provides routine uses that support these external disclosures.

[3] Additional information on the Department of Homeland Security Personnel Security Management

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

The SF-85P/86 is transmitted to OPM through the OPM secure portal. Fingerprints are shared with the FBI via the Integrated Automated Fingerprint System (IAFIS) system. Contractors and GSA are notified about suitability determinations in by email or paper copy.

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

The privacy risk associated with external sharing of the information is that the data could be lost, stolen or altered. The external sharing of information described above is consistent with the purpose of the system, which is to facilitate the background investigations of and suitability determinations for contracted service personnel. ICE shares this FPS generated PII only with organizations that have demonstrated a need to know the information in the course of their official duties. ICE has appropriate measures in place to secure the information during transit and to validate the information's accuracy before ICE takes any action that is adverse to an individual. DHS-mandated security and privacy training also mitigate the risk that FISTS users will share or handle sensitive information improperly.

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?

A Privacy Act Notice about the purposes, uses, and likely sharing of PII in CSM is provided to every individual on the Questionnaire for Public Trust Positions (SF-85P) and the Questionnaire for National Security Positions (SF-86). In addition, this PIA and the Department of Homeland Security Personnel Security Management SORN (DHS/ALL-023, Jan. 16, 2009, 74 FR 3084) SORN also provide notice.

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

Yes, but failure to provide the requested information and fingerprints is likely to result in delay or inability to complete the suitability investigation, or a finding that the individual is not suitable for the position.

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

No. By submitting the SF-85P/86, which includes an authorization and release from the individual to allow investigators to collect information from sources during the background investigation, the individual is authorizing the collection and use of his or her information for the purpose of making a suitability determination. Individuals are not required to provide the information or consent to its use, but when consent is given, it cannot be further limited by the submitter.

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.

All individuals whose PII is contained in FISTS are aware that the government is conducting a background security check on them, so the risk of individuals being unaware of the information collection are virtually non-existent. Specifically, notice is provided to individuals via the written Privacy Act Notice contained on, the authorization and release form in the SF-85P/86, this PIA, and the Department of Homeland Security Personnel Security Management SORN(DHS/ALL-023, Jan. 16, 2009, 74 FR 3084) SORN. Contractor employees and applicants expressly authorize the government to conduct a review of their financial, educational and medical background in addition to other sources of information, in order to make a determination about the loyalty, character and suitability of an individual for the position in question. Since the information is provided voluntarily by the individual and the individual has

authorized the use of their information for this purpose, there is no risk that the individual could be unaware of the collection of the information.

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?

Individuals may request access to records about them in the CSM by following the procedures outlined in the Department of Homeland Security Personnel Security Management (DHS/ALL-023) SORN. Individuals seeking access to their investigatory file must file a request directly with OPM. Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may also submit a request in writing to the ICE FOIA Office.

The Office of Personnel Management maintains the actual background investigation and individuals may request access to their background check file directly from OPM.

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

If individuals obtain access to the information in CSM pursuant to the procedures outlined in the DHS/ALL-023 SORN, they may seek correction of any incorrect information in the system by submitting a request to correct the data. The data correction procedures are also outlined in the Department of Homeland Security Personnel Security Management (DHS/ALL-023) SORN. Individuals who receive an adverse suitability determination may also file an appeal and seek to challenge the decision or the accuracy of the information upon which the decision was based. For example, the individual may present evidence such as an arrest record that was later dismissed as being invalid. Individuals can also correct information during the OPM investigative process itself if they become aware of erroneous information in the investigatory files.

In addition to the procedures above, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to:

ICE FOIA Officer

800 North Capitol Street, N.W.

5th Floor, Suite 585

Washington, D.C. 20528

Individuals may also submit requests by fax at 202-732-0310 or by email at ice-foia@dhs.gov. Please see the ICE FOIA Office's website for additional information (http://www.ice.gov/foia/index.htm). If an individual believes more than one component maintains Privacy Act records concerning him or her

the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0655, Washington, D.C. 20528.

7.3 How are individuals notified of the procedures for correcting their information?

The procedure for submitting a request to correct information is outlined in the Department of Homeland Security Personnel Security Management (DHS/ALL-023) SORN and in this PIA in Questions 7.1 and 7.2. Individuals who receive an adverse suitability determination are notified in the decision letter how to appeal that determination.

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

As stated, there is a formal appeals process for individuals who receive an adverse suitability determination. Individuals may also submit Privacy Act requests for information and correction, which will be reviewed and corrected on a case-by-case basis.

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

The privacy risk is that incorrect information will be used to make a suitability determination. However, this risk is mitigated by the fact that the individual has three potential means to access and correct information about themselves in CSM, which provides adequate redress. The first method is by correcting erroneous information during the OPM interview process. The second method is by formally appealing an adverse suitability determination. The third method is by making a formal request to access or correct their records under the Privacy Act.

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 CSM user first must be approved by their supervisor based upon a need to know for their position, to gain access the CSM. Once approved, the FISTS Administration Module supports password security control for that user. The FISTS system administrator creates a userID and temporary password for a user through the FISTS Administration Module. In addition, the user is assigned a role that governs the user's access rights. CSM user roles include: Regional Specialist, Regional Childcare Coordinator, Regional Reader, Central Office Administrator, Central Office Specialist, Central Office Childcare Coordinator, and Central Office Reader. "Central Office" users can edit all regions files and have the greatest permissions, whereas "Regional" users can only access files pertaining to their regions. "Readers" only have a view function and cannot edit. User IDs are unique to an individual and group

user IDs are not permitted in FISTS. The userID and password are used for user authentication and identification and to document user activity.

8.2 Will Department contractors have access to the system?

FPS contractors will have access to the FISTS system in order to perform their function as personnel security and certification specialists. In addition, FPS employs IT professionals that work on the FISTS system as contractors; these individuals will have access as well. Contractors are required to meet the same personnel security requirements as FPS employees.

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

All ICE personnel and contractors complete annual mandatory privacy and security training and training on Securely Handling ICE Sensitive but Unclassified (SBU)/For Official Use Only (FOUO) Information. Each government employee and contractor must be versed in acceptable rules of behavior for the system before being allowed access to the system.

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

A three-year Certification and Accreditation (C&A) was granted on August 9, 2006. FISTS is moving over to the DHS Office of Personnel Security Integrated Security Management System (ISMS) in the first quarter of FY 10.

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

Technical controls provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The FISTS application ensures that each user is authenticated before access is permitted. Each user must be approved to access FISTS applications prior to accessing the system, and assigned a role appropriate to his or her job responsibility. Logical Access Controls are built into the hardware and software features, which means that only authorized users have authorized access to or within the application to restrict users to particular transactions and functions and to detect unauthorized activities. User accounts are linked to the appropriate FISTS access control list (ACL) once the request for access has been approved. Access is restricted by the ACL to the level needed for the users to do their jobs. Access rights are strictly controlled by application roles and regional controls.

The user ID and password are used for user authentication and identification. A user has up to three attempts to logon to a FISTS application. After the third unsuccessful attempt, the application automatically locks out the user ID until the password administrator unlocks and resets the user ID. FISTS uses the password standards established in the DHS Sensitive Systems Handbook (MD 4300A).

Individual user accountability is tracked through the association of a user ID with the actions the user performs in the FISTS application.

FPS monitors the security logs regularly to detect any instance of unauthorized transaction attempts. In addition, FISTS uses SSL encryption between server and client web browsers to protect communications.

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?

A privacy risk exists in any system that stores sensitive personal data that the information will be accessed in an unauthorized manner. This risk is mitigated through various safeguards, such as access controls and the use of technological safeguards such as intrusion detection systems. Access is appropriately restricted to the level needed for users to perform their job function.

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?

FISTS is a system consisting of several modules that supports the FPS mission.

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

FISTS is in the Operation/Maintenance phase of the system lifecycle. Maintenance to the system is performed periodically and tracked for future reference.

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

No.

Responsible Officials

Lyn Rahilly
Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security