Privacy Impact Assessment
for the

FOIA/PA Information Processing System (FIPS)

DHS/USCIS/PIA-038

June 14, 2011

Contact Point
Donald K. Hawkins
Privacy Officer
US Citizenship and Immigration Services
(202) 272-8404

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

Abstract

United States Citizenship and Immigration Services (USCIS) uses the Freedom of Information Act/Privacy Act (FOIA/PA) Information Processing System (FIPS) to process Freedom of Information Act and Privacy Act requests from any person requesting access to USCIS records. FIPS uses document imaging, work flow, and web-server technologies to enable USCIS to efficiently and effectively manage the FOIA/PA case life cycle. USCIS is conducting this Privacy Impact Assessment (PIA) because FIPS uses personally identifiable information (PII) and to address major changes to the application.

Overview

The Freedom of Information Act of 1966 (FOIA), as amended (5 U.S.C. § 552), permits any person to request access to federal agency records. The FOIA establishes a presumption that records in the possession of federal departments and agencies are accessible to people, except to the extent that the records are protected from disclosure by any of nine exemptions contained in the law or by one of three special law enforcement record exclusions.

The Privacy Act of 1974 (PA), as amended (5 U.S.C. § 552a), embodies a code of fair information principles that govern the collection, use, and dissemination of PII by federal departments. The PA permits U.S. citizens and legal permanent residents (LPR) with the opportunity to request access to federal department and agency records that are maintained on an individual. USCIS manages its FOIA/PA Program in accordance with the Department of Homeland Security (DHS) policy. Any PII that is collected, used, maintained, and/or disseminated in connection with a mixed system by DHS shall be treated as a system of records subject to the Privacy Act, regardless of whether the information pertains to a U.S. citizen, LPR, visitor, or alien.[1] Individuals may request Privacy Act protected records, except to the extent that the records are protected from disclosure by exemptions or exclusions contained in the laws.

The USCIS FOIA Officer is responsible for responding to FOIA and PA requests that are submitted to the agency. USCIS uses FIPS to process such requests from any person requesting USCIS records under either of the named statutes. FIPS use document imaging, workflow, and web-server technologies to enable USCIS to manage the FOIA and PA case life cycle.

The system is maintained for the purposes of processing records requests and administrative appeals under FOIA, as well as access and amendment inquiries and appeals under PA; tracking cases in litigation arising from such requests and appeals; and assisting USCIS in carrying out any other responsibilities under FOIA or PA (i.e., preparing statutorily-mandated reports).

FIPS includes three major categories of information: PII, such as the requester's name, address, and alien number; correspondence to and from the requester and with other federal offices; and electronic images of requested USCIS records. The data includes descriptive information such as the requester's name and address and the subject of the request; indexing information such as case and document tracking numbers; and classification information such as the source and type of the request. None of the information is shared with other USCIS or DHS data systems. Only USCIS employees and contractors

[1] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf

assigned to handle FOIA and PA requests, and contractors who administer the system's technical functions, have access to the system.

Customer Service Web Portal

The Customer Service Web Portal (CSWP) provides requesters, who have submitted FOIA and/or PA requests, with the ability to check the status of their FOIA and/or PA request.[2] The requester enters the control number provided in the acknowledgment letter informing them that their request has been received. If a FOIA and/or PA request is pending, CSWP will display the date the FOIA and/or PA request was received and placement of the FOIA and/or PA request in the queue. If the FOIA and/or PA request has been processed within the past six months, the customer will be given the date the FOIA and/or PA request was processed. Requesters may check the status of their FOIA and/or PA request 24 hours a day using CSWP. The CSWP is updated daily with case status information provided by FIPS.

A typical transaction in FIPS begins when an individual submits a FOIA and/or PA request to USCIS through various communication methods including U.S. mail, electronic mail, facsimile, or the USCIS CSWP. Once received, the request is scanned into FIPS. Requests are scanned or converted into electronic images and indexed and converted into a case file that is assigned a FIPS computer generated tracking number. FOIA/PA staff then uses FIPS to generate an acknowledgment letter, which informs the requester that his/her request has been received. The acknowledgement letter also provides the requester with the FIPS computer-generated tracking number, which is used on all further correspondence concerning the request. FOIA/PA staff search for records responsive to the request by using Office of Records Services (ORS) systems, such as the National File Tracking System (NFTS) and the Central Index System (CIS). When records responsive to the request ("responsive records") are found, a request for a copy of the responsive records is forwarded to the office where the record resides. In cases where the record has been digitized, the file is downloaded from the Enterprise Document Management System (EDMS). When responsive records, for example, the A-File, are delivered to FOIA/PA staff, they are scanned into an electronic image and saved in FIPS. The FOIA/PA staff analyzes the case by reviewing, line-by-line, each page of the responsive records and redacting any information that is to be protected from disclosure according to provisions of either FOIA or PA. For PA requests, the analyst first reviews under the PA and determines what information can be provided; the analyst then reviews under FOIA to ensure the individual receives as much information as possible about him or herself. After a final review of the case file by a senior analyst is complete, FOIA/PA staff use FIPS to generate a letter to the requester itemizing the records and identifying what, if any, exemptions were used to withhold portions of the record. FIPS can either print the responsive records on paper or, if lengthy or requested by the requester, save to a compact disk. When no records responsive to the request exist, the component sends a letter to the requester advising them accordingly.

The authority to collect information in FIPS is set forth in the Freedom of Information Act, as amended (5 U.S.C. § 552), the Privacy Act of 1974 as amended (5 U.S.C. § 552a), Departmental Regulation 6 C.F.R. Section 5.1, and Records Management by Federal Agency Heads (44 U.S.C. § 3101). Information processed using FIPS may be shared within DHS, as well as with appropriate federal, state, local, tribal, foreign, or international government agencies.

[2] To check the status of a FOIA and/or PA request, please see www.uscis.gov.

In a future release of FIPS, requests submitted through CSWP will be electronically transmitted into FIPS. USCIS will update this PIA to document system enhancements as FIPS matures to address associated privacy risks and mitigation.

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?

The PII that individuals submit with their FOIA and/or PA requests to USCIS depends on the substance of the request.

USCIS may collect the following searchable information:

- Requestor and Subject of Record Name(s);
- Requestor Business and/or Personal Address(es), as applicable;
- Requestor Business and/or Personal Phone Number(s), as applicable; and
- Subject of Record Alien Number (A-Number), as applicable.

For PA requests specifically, when individuals seek records from this system of records or any other departmental system of records, their request must conform with the Privacy Act regulations set forth in 6 CFR part 5. Individuals must first verify their identity, meaning that they must provide their full name, current address, and date and place of birth. Individuals must sign their request and their signature must be either notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. USCIS does not request SSNs and individuals are not required to submit such information.

FIPS also maintains records responsive to FOIA/PA requests in a non-searchable format. This information may include the following data elements: names, addresses, phone numbers, facsimile numbers, zip codes, email addresses, A-numbers, social security numbers (SSN), other identifying numbers, fingerprints, date of birth, country of birth, mother's maiden name, birth records, marriage records, passport records, death records, tax records, civil or criminal history information, biometric identifiers, and/or photographic facial images.

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

The sources of information for FOIA and/or PA requests are:

- Individuals who submit FOIA and/or PA requests;
- Individuals who appeal USCIS' denial of their FOIA and/or PA requests;

- Individuals whose requests, appeals, and records were referred to USCIS by other agencies; and
- Attorneys or other persons representing the individual submitting such requests and appeals.

The sources of the information for responsive records can be from a variety of systems of records, including the Alien File (A-File), Enterprise Document Management System (EDMS), Central Index System (CIS), and National File Tracking System (NFTS).[3]

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

USCIS uses this information to efficiently and accurately process record requests and administrative appeals under FOIA and PA. USCIS also uses this information for litigation purposes arising from such requests and appeals; and in assisting USCIS in carrying out any other responsibilities under FOIA or PA, including reporting requirements such as the Annual FOIA Report to the U.S. Attorney General.

1.4 How is the information collected?

Individuals provide information to USCIS when submitting FOIA and/or PA requests. Requests are received through various communication methods including U.S. mail, electronic mail, facsimile, or the USCIS CSWP. Requests are scanned or converted into electronic images and indexed and converted into a case file. In a future release of FIPS, requests submitted through CSWP will be electronically transmitted into FIPS.

USCIS collects records responsive to the request from the appropriate USCIS Directorate and scans into FIPS. Digitized records are obtained electronically from EDMS and stored in FIPS.

1.5 How will the information be checked for accuracy?

Information received by USCIS from individuals submitting FOIA and/or PA requests is assumed to be true and accurate unless follow-up documentation or correspondence indicates otherwise. There are three levels of review that take place to ensure accuracy of information entered into FIPS. First, USCIS FOIA/PA administrative staff compares the information contained in the original request letter against the information contained in CIS. Second, a FOIA/PA analyst reviews and confirms that the PII contained in the responsive record matches the identifying information provided by the requester. This level of review is to assure that the correct requested record has been scanned into FIPS. Lastly, before a response is sent to the requester, all of the information and records are reviewed for accuracy by a FOIA/PA senior analyst.

Should any inaccuracies be discovered during the resolution of the case file, USCIS may contact the originating submitter for clarification.

[3] For additional information, please see DHS-USCIS-001 – Alien File (A-File) and Central Index System (CIS) SORN at www.dhs.gov/privacy.

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

USCIS is authorized to collect this information per The Freedom of Information Act of 1966, as amended (5 U.S.C. § 552), the Privacy Act of 1974 as amended (5 U.S.C. § 552a), Departmental Regulation (5 U.S.C. § 301), and Records Management by Federal Agency Heads (44 U.S.C. § 3101).

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: Non-essential information may be collected.

Mitigation: To mitigate this risk, USCIS only requires certain information when an individual submits a request, such as name, date, place of birth, physical address, and FOIA and/or PA request information. If the individual provides more information than necessary, USCIS will redact and protect this information and will not enter the extraneous information into the applicable FOIA and PA system. This information will remain in the paper file but will not be further disseminated.

Privacy Risk: Information may be inaccurate.

Mitigation: The risk of inaccuracy is reduced by collecting contact information directly from the individual requester or representative. FOIA and PA depend on the originating office for the accuracies of the responsive record. Information entered into FIPS undergoes three levels of review to ensure the accuracy of information.

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.

Information received by USCIS from individuals submitting FOIA and/or PA requests may be used to assist USCIS in conducting a search for the requested record. When no records exist that are responsive to the request, USCIS sends a letter to the requester advising them accordingly.

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

The Commercial-Off-The-Shelf (COTS) package Crystal Reports is used to analyze data. A variety of reports are produced to manage staff productivity, respond to queries by DHS and USCIS upper management, and provide USCIS data for inclusion in the statutorily-mandated DHS Annual Report to the Attorney General of the United States. Management reports may contain PII. In addition, FOIA logs generated by the reporting tool may also contain PII.

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

FIPS does not use 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: Access to information may be unauthorized.

Mitigation: The information contained in FIPS is used for the purpose of responding to FOIA and/or PA requests. Access to FIPS is only given to users who need it to perform their work. In addition, all users must be authenticated by user ID and passwords. Only FOIA and PA personnel and USCIS contractors have access to the FIPS information. Only those users with approved and assigned roles can search and process data and document images associated with any particular request.

Privacy Risk: Information may not b used for its intended purpose.

Mitigation: FOIA and PA personnel and their contractors are required to complete Computer Security Awareness Training, Privacy Act Training, and Records Management Awareness Training annually. All of the training programs address the responsibility of using USCIS data and records for their intended purposes only. In addition, DHS components are ultimately responsible for ensuring that data is used appropriately. This is done by the establishment of standard operating procedures that stipulate prescribed and permitted activities, uses, auditing requirements, and integrity controls.

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?

All information identified in Section 1.1 above is retained.

3.2 How long is information retained?

Records pertaining to FOIA and/or PA requests are retained and disposed of in accordance with the National Archive and Records Administration's (NARA) General Records Schedule (GRS) 14. Files may be retained for up to six years. Requests that result in litigation are retained for three years after final court adjudication.

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

Yes, records pertaining to FOIA and/or PA are retained and disposed of in accordance with the NARA's GRS 14.

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

Privacy Risk: Data may be retained longer than necessary.

Mitigation: Records maintained in FIPS are retained and disposed of in accordance with NARA's GRS 14. 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. This adheres to requirements of the DHS Information Technology Security Programs Handbook to include the issuance and use of password protection identification features. All internal components are mandated by DHS to comply with DHS' Sensitive System Security guidelines.

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?

Documents may be shared with DHS, Immigration and Customs Enforcement (ICE), and Customs and Border Protection (CBP) in order for these components to respond to FOIA and/or PA requests. Annual summaries and statistical data that do not include PII are shared with DHS for the purpose of the statutorily mandated DHS Annual Report to the Attorney General **(**i.e., Annual FOIA and PA Report).

4.2 How is the information transmitted or disclosed?

Spreadsheets and word processing documents that contain annual summaries and statistical data are uploaded to Sharepoint for access by the DHS Privacy Office. Referral documents that may contain PII are sent by electronic mail or printed and sent by first class mail to the appropriate component.

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: Personal information may be inappropriately accessed or misused.

Mitigation: Access to FIPS is restricted to authorized personnel who need access to perform their particular job functions. The completion of appropriate access agreements is required for all individuals requiring access prior to access being authorized. All individuals are mandated by USCIS policy to comply with Sensitive System Security guidelines. All individuals are also required to complete mandatory Security Awareness, Privacy Act Training, and Records Management Awareness Training.

FIPS has a comprehensive audit tracking and maintenance function that stores information on each action performed within the application to prevent misuse of data. All user actions are tracked via audit logs, including date, time, and data accessed.

The Sharepoint Administrator customizes user access to authorized individuals with a need to know the information. Disclosure of the information in this system is only permitted to authorized individuals in the performance of their official duties.

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?

A portion or all of the information maintained in FIPS may be shared with the following:

- The Department of Justice (DOJ), including United States Attorney Offices, or other federal agencies conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation;
- A congressional office in response to an inquiry made at the request of the individual to whom the record pertains;
- A federal agency or other federal entity that furnished the record or information for the purpose of permitting that agency or entity to make a decision regarding access to or correction of the record or information, or for purposes of providing guidance or advice regarding the handling of particular requests;
- An agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function; and

- Federal, state, tribal, local, international, or foreign agencies, including law enforcement or other appropriate authorities charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations, and such disclosure is proper and consistent with the official duties of the person making the disclosure.

In addition to those disclosures generally permitted under 5 U.S.C. § 552a (b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS in accordance with the routine uses found in DHS/ALL-001 - Freedom of Information Act and Privacy Act Record System.[4]

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.

The external sharing is compatible with the original collection. USCIS shares information with external organizations when required by statue, executive order, regulation, or policy and for the response of a FOIA and/or PA request. These instances of sharing are fully consistent with the DHS/ALL-001 - Freedom of Information Act and Privacy Act Record System.

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

Documents are printed and sent by mail to the appropriate external agency. The material is mailed in accordance with DHS procedures. The information is sealed in an opaque envelope or container and mailed using U.S. Postal Service's First Class Mail, Priority Mail, or an accountable commercial delivery service.

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 maintained in FIPS.

Mitigation: To mitigate this risk of unauthorized disclosure, information is shared only with external agencies under the applicable provision of DHS/ALL-001 - Freedom of Information Act and Privacy Act Record System.

[4] For additional information, please see DHS/ALL-001 – Department of Homeland Security (DHS) Freedom of Information Act (FOIA) and Privacy Act (PA) Record System SORN at www.dhs.gov/privacy.

No external users are authorized access to FIPs. Information that is shared is printed and mailed to external agencies using the U.S. Postal Service's first class mail or priority mail, or an accountable commercial delivery service.

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?

Notice is given by the Privacy Act Notice, which is available on USCIS forms and/or associated webpage. Notice is also provided in the Federal Register by the published DHS/ALL-001 - Freedom of Information Act and Privacy Act Record System. In addition, notice is also provided by this PIA. FIPS is not the original point of collection for PII data in responsive records. Notice for responsive records is provided at the original point of collection.

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

Submission of a FOIA/PA request is strictly voluntary. Requesters can decline to provide information, however; the information about the requester is required to process a FOIA and/or PA request. In instances of the responsive records, the right to decline is given at the point the individual submitted the information for a benefit.

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 information is strictly voluntary. The individual does not have the right to consent to particular uses of the information.

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 may not be provided with sufficient notice of the collection and use of their information.

Mitigation: Requesters are given notice through the publication of the DHS/ALL-001 - Freedom of Information Act and Privacy Act Record System and this PIA.

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?

All requests for access must be made in writing. For those individuals subject to the Privacy Act, proper identification (a notarized signature or submitted sworn statement under penalty of perjury) must be included. Requesters are required to provide their full name, date and place of birth, and return address.

Individuals may request access to their information by submitting a request to USCIS in writing at the following address:

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?

To update or correct their mailing address, requesters can submit an address change form to the above address. Requests for correction of responsive records under the PA are directed to the FOIA/PA Office as noted in section 7.1.

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

DHS/ALL-001 - Freedom of Information Act and Privacy Act Record System provides individuals with procedures for correcting their information.

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

Formal redress is provided to individuals in accordance with the above sections.

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: Individuals may not have knowledge of how to access or amend their records.

Mitigation: The risk is mitigated by providing individuals guidance on how to access and amend their records through the DHS/ALL-001 - Freedom of Information Act and Privacy Act Record System and this PIA.

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?

Access to FIPS is on a need-to-know basis. The need to know is determined by the individual's current job function. FIPS users are granted access to FIPS following standard USCIS procedures for obtaining security clearances, active directory user identification names, and access to individual USCIS systems. FIPS users are assigned roles which limit access to data only as needed to fulfill their job functions.

8.2 Will Department contractors have access to the system?

USCIS contractors have access to FIPS in order to provide continuing operation and maintenance support. This includes providing system administration for all servers and associated devices, design, and development for USCIS management system change requests, as well as integration and deployment of upgraded or new hardware and/or software.

USCIS contractors, under the direction of the local offices that use FIPS, are granted access to FIPS following standard USCIS procedures for obtaining security clearances, password issuance control system user identification names, and access to individual USCIS systems. Such contractors are assigned roles by the local office to perform tasks including scanning documents, creating cases, processing cases and printing correspondence.

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

All FIPS users complete the mandatory annual Computer Security Awareness, Privacy Act, and Records Management Awareness training. All trainings include guidance on federal laws, policies, and regulations relating to privacy, data integrity, and the handling of "Sensitive" but "Unclassified/For Official Use Only" information. USCIS Office of Information Technology System 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?

FIPS completed its Certification and Accreditation November 8, 2010 and has an Authority to Operate until November 8, 2011.

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

FIPS has a comprehensive audit trail tracking and maintenance function that stores information on each action performed within the application to prevent misuse of data. FIPS audit capabilities include the tracking of all user actions via audit logs to identify information by user, date, time, and data accessed.

The FIPS business owner and Information System Security Officer routinely reviews user lists and has the computer system administrator disable inactive accounts where necessary.

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?

Privacy Risk: There may be unauthorized access to information.

Mitigation: Access and security roles have been established to mitigate privacy risk. Access to FIPS is limited to authorized users. All users must possess valid user IDs and passwords to access the system.

Privacy Risk: Non-authorized users may have indirect access to personal information.

Mitigation: FIPS system administrators and managers monitor FIPS to ensure only authorized users have access to information contained in FIPS. No guest accounts are ever created in FIPS. FIPS system administrators follow USCIS standard transfer and termination procedures to ensure that system accesses are revoked on employees or contractors who leave USCIS or are reassigned to other duties for which access is no longer required. FIPS managers review audit records for inappropriate activities in accordance with USCIS procedures. Downloading and the storage of PII outside of the FIPS system is not permitted. The application locks users out after 20 minutes of inactivity. In addition, system administrators disable accounts when access is no longer needed.

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?

FIPS is an operational product and a software application that consists of the integration and configuration of several COTS products.

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

FIPS is in the operations and maintenance phase with FIPS 7 as a major release. The development of FIPS and the continuing corrective and adaptive actions follow 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.

FIPS does not employ technology which may raise privacy concerns.

Responsible Officials

Donald Hawkins, Privacy Officer

United States Citizenship and Immigration Services

Department of Homeland Security

Approval Signature Page

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan

Chief Privacy Officer

Department of Homeland Security