Privacy Impact Assessment
for the

Immigration Benefits Background Check Systems

November 5, 2010

Contact Point
Donald Hawkins
USCIS Privacy Officer
United States Citizenship and Immigration Services
202-272-8000

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

Abstract

As part of its benefits adjudication process and as required by law, the United States Citizenship and Immigration Services (USCIS) conducts background checks on petitioners and applicants who seek certain immigration benefits. These background checks consist of four separate checks against systems within Department of Justice (DOJ), Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS). In order to facilitate the collection and transmission of information necessary to complete background check processes, USCIS maintains five information technology electronic systems: the Fingerprint Masthead Notification System (FMNS), the Customer Identity Capture System (CICS), the FD-258 Tracking System - Mainframe (FD-258 MF), the Benefits Biometrics Support System (BBSS), and the Interagency Border Inspection System (IBIS) Manifest. USCIS is conducting this privacy impact assessment (PIA) because FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest collect, use, and share personally identifiable information (PII). This PIA replaces the previously published USCIS PIA for the "Background Check Service (BCS)" which describes planned background check-related systems that were never implemented. Upon publication of this PIA, the BCS PIA will be retired.

Introduction

Title 8 U.S.C. § 1101 et seq. requires background checks to be conducted for certain immigration benefits. The background check process is triggered as soon as the petitioner or applicant (hereafter collectively referred to as "applicants") applies for a benefit. In adjudicating applications for benefits, USCIS conducts four different background checks, two biometric fingerprint-based and two biographic name-based.

After an applicant submits a USCIS application for which a background check is required, USCIS contacts the applicant by mail with an appointment time to have his biometrics taken at a specified USCIS Application Support Center (ASC).[1] At the ASC, USCIS electronically captures the applicant's fingerprints (hereafter referred to as "the 10-prints") and related biographic data.

This PIA replaces the previously published USCIS PIA for the BCS describing planned background check-related systems that were never implemented. USCIS continues to operate five information technology systems in collecting biometrics and processing the background checks: FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest.[2] USCIS is developing a single system to streamline the

[1] USCIS implemented additional processes in response to the Kendall Frederick Citizenship Assistance Act. Public Law 110-251. The process allows USCIS to accept fingerprints previously submitted by military citizenship applicants at the time of their enlistment or from prior submissions to DHS. The Act applies to only those individuals applying for naturalization within 24 months of military enlistment. This expedites the processing of military applicants applying for citizenship.

[2] Systems used to support case management and application adjudication are covered in separate PIAs available at www.dhs.gov/privacy, most notably the September 5, 2008 *USCIS Benefits Processing of Applicants other than Petitioners for Naturalization, Refugee Status, and Asylum (CLAIMS 3)* and *USCIS Computer Linked Application Information Management System (CLAIMS 4)*.

process and to limit the privacy risks associated with using multiple systems. USCIS will issue a new PIA once the technology has been developed.

Background Check Processes

USCIS uses background check results to assist in determining an applicant's eligibility for a benefit. If the background check result from the FBI or DHS yields an item of law enforcement or national security interest, USCIS may work with DHS Customs and Border Patrol (CBP), the FBI, or other law enforcement entities, such as Immigration and Customs Enforcement (ICE), to determine whether law enforcement actions should be pursued.

The four background checks are:

- two biometric fingerprint-based:
    1. the FBI Fingerprint Check;
    2. the US-VISIT's Automated Biometric Identification System (IDENT) Fingerprint Check;
- two biographic name-based:
    3. the FBI Name Check; and
    4. TECS Name Check.

Five IT systems support the background check processes identified above: FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest.

1. FBI Fingerprint Check

The FBI Fingerprint Check is conducted on applicants over the age of 14 when the benefit allows them to remain in the United States beyond one year. The FBI Fingerprint Check is a search of the FBI's Integrated Automated Fingerprint Identification System (IAFIS) to identify applicants who have an arrest record. IAFIS[3] is a national fingerprint and criminal history system maintained by the FBI's Criminal Justice Information Services (CJIS) Division. The applicant's fingerprints are processed by the FBI pursuant to an Interconnection Security Agreement (ISA) between the FBI and USCIS.

The FBI electronically sends responses to USCIS indicating whether there is a criminal history response. If there is a criminal history record, FBI also sends the FBI Record of Arrests and Prosecutions[4] (commonly referred to as the "RAP Sheet") to USCIS electronically. The RAP Sheet is stored in BBSS. A hard copy of the RAP Sheet is also sent to the respective service center and is stored

[3] For FBI's related privacy documentation, see the IAFIS and DOJ/FBI Interim Data Sharing Model PIAs at http://foia.fbi.gov/iafis.htm, and http://foia.fbi.gov/idsm.htm, respectively and corresponding SORN for the FBI Fingerprint Identification Records System (FIRS)(JUSTICE/FBI-009) (64 FR 52343, 52347; 66 FR 33558; 70 FR 7513, 7517; 72 FR 3410 and associated blanket routine uses at 66 FR 33558 and 70 FR 7513-02) which can be found at http://foia.fbi.gov/firs552.htm.

[4] The RAP Sheet is a listing of certain information taken from fingerprint submissions retained by the FBI in connection with arrests and, in some instances, includes information taken from fingerprints submitted in connection with federal employment, naturalization, or military service.

in the applicant's Alien file (A-File).[5] The RAP Sheet includes the name of the agency or institution that submitted the fingerprints to the FBI, the date of arrest and the date the individual's fingerprints were received by the agency submitting the fingerprints, the arrest charge, and the disposition of the arrest if known by the FBI. All arrest data included in a RAP Sheet are obtained from fingerprint submissions, disposition reports, and other reports submitted by agencies having criminal justice responsibilities.

2. IDENT Fingerprint Check

The IDENT fingerprint check is conducted on applicants over the age of 14 when the benefit allows them to remain in the United States beyond one year. IDENT is the official DHS-wide system for the biometric identification and verification of individuals encountered in DHS mission-related processes. The 10-prints are enrolled and stored to check for matches. If there is derogatory information, that information is emailed to USCIS via an encrypted spreadsheet. The spreadsheets, emailed on a weekly basis, may contain information on more than one applicant. IDENT results may include known suspected terrorists and other national security and/or public safety concerns. IDENT search results are stored in IDENT and not stored in BBSS.

3. FBI Name Check

The FBI Name Check is conducted on applicants over the age of 14. The FBI Name Check is a name-based search of the FBI's Central Records System (CRS) and Universal Index (UNI).[6] The CRS encompasses the centralized records of FBI Headquarters, FBI field offices, and Legal Attaché offices. The CRS contains FBI investigative, administrative, criminal, personnel, and other files compiled for law enforcement and national security purposes. The UNI consists of administrative, applicant, criminal, personnel, and other law enforcement files. USCIS sends applicant information (name, date of birth (DOB), country of birth, race, and gender) to the FBI in order to conduct the name check. The secure data exchange between USCIS and the FBI for the purpose of FBI Name Check occurs via zipped and encrypted email.

The UNI is searched for "main files," files where the name of an individual is the subject of an FBI investigation, and for "reference files." Reference files are files where the name being searched is merely mentioned (not as the main subject) in an investigation.

The FBI will respond to the FBI Name Check with either a: "no record," "positive response," or "pending." A no record response means that the FBI has no relevant information based on the name and DOB of the applicant. A pending response means further research is needed before the FBI can provide a final response. For those records with an initial response of pending, the FBI will complete a review of their records and provide a final response of no record or positive response. A positive response means the FBI has information relating to the name submitted. The FBI sends the actual information in a Letterhead Memorandum relating to the positive response separately via encrypted email or over the classified network. The memoranda are stored in the A-File and if the memoranda are classified, then the A-File becomes classified. Records for refugees are stored in FD-258 MF.

[5] DHS/USCIS-001 Alien File (A-File) and Central Index System (CIS) System of Records Notice (72 FR 1755).
[6] DOJ/FBI Central Records System (66 FR 29994)

4. TECS Name Check

The TECS Name Check is conducted on all applicants over 14 years of age. The TECS [7] Name Check query consists of a name-based search of a multi-agency database containing information from 26 different federal agencies. The information in TECS includes records of known and suspected terrorists, sex offenders, people who are public safety risks and other individuals that may be of interest (e.g., individuals who have warrants issued against them, people involved in illegal gang activity, etc.) to the law enforcement community. If there are positive results from the TECS Name Check, the results are stored in IBIS Manifest and may be placed in the A-File.

USCIS Background Check IT Systems

There are five IT systems that support the background check process outlined above: FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest.

1. FMNS

FMNS is a stand-alone system that runs on a computer desktop at the ASCs. The data in FMNS is automatically deleted 60 days after it is captured. FMNS is only used when the electronic systems for capturing fingerprints, commonly referred to as the livescan device, are not functioning, when the ASC is extremely busy, or if the livescan device is not suitable for capturing fingerprints for example, because of accessibility for accessibility reasons. In these instances a hard copy of fingerprints needs to be printed and submitted. When this occurs, the 10-prints and biographic data are collected on the paper-based FD-258 card. The biographic data is entered into FMNS and printed on the FD-258 card. These cards are mailed to the service centers. The completed FD-258 cards are then scanned and uploaded into BBSS and the electronic fingerprint transmission specification (EFTS) record is forwarded to the FBI where the 10-print criminal background check is conducted.

FMNS maintains FD-258 masthead data, applicant's name, address, DOB, Social Security number (SSN) (if available), Alien Number (A-Number), country of birth, country of citizenship, current address, aliases, gender, race, height, weight, eye color, and hair color. FMNS creates a manifest of FD-258 cards printed and generates letters to notify applicants of the time and place where they need to appear to provide fingerprints.

2. CICS

The CICS application resides on USCIS configured laptops that have a fingerprint scanner and camera. CICS is used to capture biographic, biometric and photo image information in refugee camps and in USCIS overseas offices from applicants seeking immigration benefits from USCIS. CICS transmits applicant data into the BBSS.

3. FD-258 MF

The FD-258 MF record contains biographic data, fingerprint transmission data, and fingerprint response data. This record is stored to assist in the adjudication process. If there is a RAP Sheet, it is not sent to FD-258 MF. As noted above, the RAP Sheet is sent separately and stored in the paper A-File.

[7] DHS/CBP-011 U.S. Customs and Border Protection TECS (73 FR 77778).

4. BBSS

In 1999, USCIS developed BBSS[8] to process fingerprints taken electronically at the ASC and transmits them to the appropriate USCIS SC for processing. BBSS receives fingerprints taken at the ASCs or at refugee camps and USCIS oversees office through CICS and forwards them to one of four USCIS service center where the 10-print records are encrypted and electronically transmitted to the FBI for the FBI Fingerprint Check.

BBSS also facilitates the transfer of biometric and biographic data pursuant to the United Kingdom (UK) Visa Program, which is covered by a separate PIA.[9]

BBSS maintains information on the FBI Fingerprint Check.

5. IBIS Manifest

USCIS developed IBIS Manifest to conduct TECS Name Checks against TECS. The results of the name check search are stored in IBIS Manifest for adjudication purposes. USCIS adjudicators have access to the results in this system to determine an applicant's eligibility for the immigration benefits being sought.

To initiate a name check, adjudicators either wand-in or manually enter the applicant's receipt number into IBIS Manifest. IBIS Manifest uses the receipt number to retrieve the applicant's full name, DOB, A-Number, and benefit form-type from the Citizenship and Immigration Service Centralized Oracle Repository (CISCOR) either via a user interface or through a batch submission process. The applicant's data is then electronically transmitted to TECS to perform a background check. The investigation yields results of either "hit" or "no hit" based on the applicant's full name and DOB. The name check results are received by and stored in IBIS Manifest. A history action code is placed in Computer-Linked Application Information Management System (CLAIMS 3) if there is no derogatory information. If derogatory information is returned, the "hit" result is all that is stored in CLAIMS 3. The adjudicator must log into TECS to view the derogatory information.

Results of Background Checks

Depending upon the nature of the benefit requested, the indicator response will be maintained in the following benefit case management systems:

- CLAIMS 4, for naturalization applications;
- Refugees, Asylum, and Parole System (RAPS), for asylum applications, and
- Marriage Fraud Assurance System (MFAS) for the TECS Name Check.
- Paper copies may also be maintained in the A-File.

[8] In 2000, a new website was added that provides users with the ability to query and view records stored in BBSS.

[9] DHS/UK Visa Project, November 14, 2007 found at:
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_ukvisa.pdf

These systems maintain an indication that the background checks have been run for the relevant benefit being requested.

Results of Background checks are maintained as follows:

1. FBI Fingerprint Checks – BBSS maintains copies of the responses to the FBI Fingerprint Check and the FBI RAP Sheets. In certain instances, the RAP Sheets will also be placed in the A-File.
2. IDENT Fingerprint Checks – IDENT maintains the results.
3. FBI Name Check – The no records, pending, or positive response codes are stored. Positive responses are sent to the National Benefits Center (NBC) on Letterhead Memoranda in encrypted format and printed and placed in the A-File. If the response is a national security or public safety issue, the response is maintained in Fraud Detection National Security-Database System.
4. TECS Name Check – This check is stored in IBIS Manifest and may be placed in the A-File. Also, a history action code is placed in CLAIMS 3 if there is no derogatory information.

This PIA covers the IT systems that support the fingerprint process from collection at the ASC or through CICS to completion, when results are received. In order to understand the entire process of background checks, the introduction in this PIA is necessarily more comprehensive. The remainder of this PIA will concentrate only on the five IT systems: FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest.

Section 1.0 Information collected and maintained

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

1.1 What information is collected?

The information collected and stored in FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest includes biographic and biometric data provided by applicants at the ASC (or scanned from FD-258 cards in certain situations), refugee camps and oversees or from the application or petition submitted when seeking a USCIS benefit.

An applicant's 10-prints, photo, signature and an index finger press-print are collected at the USCIS ASCs using livescan machines that interface with BBSS or at refugee camps and oversees using CICS , which is a mobile laptop unit. The 10-prints are stored in IDENT and at the FBI.

FMNS

FMNS collects and temporarily stores the following information for 60 days: applicant's name (first, last and middle), address, reason fingerprinted, DOB, aliases, A-Number, reason for fingerprint, SSN, country of birth, country of citizenship, gender, race, weight, height, eye color, and hair color.

CICS

CICS collects and temporarily stores A-Number, SSN, name, DOB, country of birth, country of citizenship, sex, race, height, weight, eye color, hair color, alias, residence address, city, state, and zip code of person fingerprinted, Originating Agency Identification (ORI) Code, SC ORI Code, destination SC ORI Code, reason fingerprinted, site code, Z-number, a single photograph image, and a full set of 10-print fingerprint images.

FD-258 MF

The data stored in FD-258 MF includes:

Biographic Data: applicant's name (last, first, middle), SSN (if the applicant provides it, as SSNs are not required), two additional SSN fields for applicants who provide more than one (in the case of an applicant fraudulently or accidentally using more than one SSN), street address, city, state, ZIP code, up to five aliases, country of citizenship, DOB, two additional DOBs, sex, race, height, weight, eye color, hair color, country of birth, A-Number.

Fingerprint Data: Transaction Control Number (TCN), fingerprint service requested (criminal background check), date fingerprints were sent to the FBI, miscellaneous number (e.g., Z Number[10]), date/time fingerprints were taken, reason fingerprinted (represented by USCIS form type), ASC site code, ASC machine ID, ASC employee ID, ORI code (i.e., District Office (DO) ORI, SC ORI code), and external system ID (e.g., A-Number for CLAIMS 4, receipt number for CLAIMS 3).

Fingerprint Result Data: TCR, FBI response, date processed by the FBI, date processed by the SC, date processed by FD-258 MF, and FBI Number (number assigned to a record with a RAP Sheet).

While all of the data mentioned above is stored in the FD-258 MF database, only the following information is displayed for the user to view: A-Number, name, service center ORI, DOB, TCN, TCR, country of birth, FBI response, date processed by the FBI, date processed by the service center, date processed by FD-258 MF, and FBI Number.

BBSS

Records in BBSS related to the FBI Fingerprint Check include the following information:

Biographic Data: name (last, first, middle), may include SSN, two additional SSNs in the event that the applicant is using multiple SSNs either fraudulently or accidentally) street address, city, state, ZIP Code, up to five aliases, country of citizenship, DOB, two additional DOBs, sex, race, height, weight, eye color, hair color, place of birth, and A-Number.

Fingerprint Data: TCN - a unique number generated by the live scan device, fingerprint service requested (criminal background check), date fingerprints were sent to the FBI, miscellaneous number (e.g., Z Number), date/time fingerprints were taken, external system ID (e.g., CLAIMS 3, and CLAIMS 4), external system ID, reason fingerprinted (represented by form type), ASC site code, ASC machine ID, ASC employee ID, Local ORI code (i.e., DO ORI), service center ORI code).

[10] A Z Number is a temporary ID number used when no other identifying number is provided.

Fingerprint Result Data: TCR - a unique number assigned to each transaction by the FBI, and the RAP Sheet (where one exists). If there is no match in IAFIS, the FBI's response is "NON-IDENT" which is stored in BBSS and FD-258 MF. If a criminal history record does not exist, the FBI provides USCIS a response (NON-IDENT) indicating that there was not a match on the fingerprints submitted.

The image sets (press-print, photo and signature) captured at the ASCs are transferred through BBSS for use in card production. Images related to cards that have been produced are stored in the Image Storage and Retrieval System (ISRS) which will retire at the end of the fiscal year and be replaced by Customer Profile Management System (CPMS) but the information is not stored in BBSS. [11] This information that passes through BBSS includes the receipt number and the image set.

IBIS Manifest

IBIS Manifest collects and stores the following information: full name (first, middle, and last), aliases, DOB, A-Number, receipt number, benefit form type, and TECS Name Check results ("HIT" or "NO HIT").

1.2 From whom is information collected?

The biometric information provided by the applicant for the FBI Fingerprint Check and the IDENT Fingerprint Check is taken from the livescan application at the ASC. The biographic information is collected from the applicant at the time the fingerprints are taken. Fingerprints are taken at one of USCIS' ASC and sent electronically to one of the USCIS service centers. If the applicant is unable to have their fingerprints taken by one of the electronic livescan fingerprint capture devices, a hard copy fingerprint card (FD-258 card) is used to capture the fingerprints and that hard copy is mailed to one of the service centers. The hard copy FD-258 is scanned into an electronic format at the service center. All fingerprints are encrypted and sent to the FBI electronically. The responses to the FBI Fingerprint Check are encrypted and sent back to USCIS electronically from the FBI and the results are stored in FD-258 MF. The biographic information used for the FBI Name Check and the TECS Name Check is taken from the application/petition submitted by the petitioner or an authorized representative.

In addition, CICS captures biographic, biometric, and photo image information primarily of refugees and beneficiaries of I-730 petitions (V92/93) who are considered for refugee status in the United States in accordance with U.S. Law and international mandates; and also for applicants, petitioners, and beneficiaries applying in USCIS overseas offices for USCIS benefits including eligibility for certain types of non-immigrant and immigrant visas, naturalization, travel documents, waivers, and parole.

The biographic information from the application/petition is entered into one of USCIS' case management systems. The USCIS case management systems include:

- CLAIMS 3, which is used to process applications for benefits other than naturalization, refugee, and asylee status;

[11] For a detailed discussion of ISRS and ICPS, please see *Privacy Impact Assessment for the USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum* (September 5, 2008), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_claims3.pdf.

- CLAIMS 4, which is used to process applications for naturalization;
- CISCOR, which is used to consolidate and maintain an exact replica of CLAIMS 3 data;
- RAPS, which is used to process Asylum applications; and
- MFAS, which is used for processing information relating to investigations of marriage fraud.

1.3 Why is the information being collected?

The collection of information is required to conduct the background check required by 8 U.S.C. § 1101 *et seq*. and to produce USCIS issued documents for applicants who have been approved for the respective benefit. The background checks are conducted to determine if information is available from FBI IAFIS, US-VISIT IDENT, FBI Name Check or TECS Name Check that would make the applicant ineligible for the benefit sought. USCIS cannot grant certain benefits unless it collects the information necessary to meet this statutory requirement.

The image set (press-print, photo, and signature) is collected and is put on the UCSIS issued documents including the Permanent Resident Card (PRC), Employment Authorization Document (EAD), Re-Entry Permit (REP), and Refugee Travel Document (RTD).

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

The legal authority to collect this information is derived from 8 U.S.C. § 1101 *et seq*. (Aliens and Nationality).

In addition, the U.S. Office of Management and Budget (OMB) approves the format of every public form utilized by USCIS to collect the information in conjunction with requested immigration benefits through the Paperwork Reduction Act process.

USCIS has signed an ISA and MOU with the FBI that set forth the terms and conditions for the transfer and use of information pertaining to background checks and associated with the interaction with BBSS, FMNS and FD-258 MF (via BBSS). USCIS has an MOU with US-VISIT covering the biometric and biographic information sharing. *MOU between U.S. Citizenship and Immigration Service Department of Homeland Security and US VISIT U.S. Department of Homeland Security and Bureau of Customs and Border Protection U.S. Department of Homeland Security for the Purpose of Sharing Relevant Biometric and Biographic Data (Travel Document and Ten-Print Fingerprint Data for the US VISIT Increment 2A Program, December 16, 2005).*

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

Privacy Risk: The overarching risks presented by the current USCIS background check processes and systems stems from the very complex and outdated technology used. The main risk is that the technologies will fail.

Mitigation: These risks will not be fully mitigated until USCIS is able to replace these older mainframe systems with an appropriately up-to-date Information Technology (IT) solution. USCIS is in the first year of a five year comprehensive transformation initiative that includes replacing the existing systems with a technical solution that incorporates the latest data security practices. In the interim, USCIS employs standard operating procedures to keep records of background check responses, such as printing responses in hardcopy to be filed in the applicant's permanent A-File record.

Privacy Risk: Misuse and inappropriate dissemination of data.

Mitigation: USCIS has implemented measures to mitigate these risks in the design of FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest by limiting access to these systems to authorized personnel who need this information to make an adjudication decision.

USCIS developed and implemented FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest in accordance with DHS approved security guidelines. Only users who need the information to effectively perform their job functions are granted access to FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest. These authorized users must go through an approval process and can only access FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest through DHS approved equipment. All USCIS adjudicators who use FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest during the adjudication process are required to take the annual security awareness and Privacy Act training.

Privacy Risk: Inherent in the use of multiple systems for background check processing is the unnecessary duplication of data and the risks to control data when it exists in so many instances.

Mitigation: USCIS recognizes this risk and is developing a centralized system for storing and managing all biometrics and background check activity. This new system is part of the broader "Transformation Initiative" mentioned above.

Privacy Risk: Lack of transparency.

Mitigation: Transparency into the background check process is difficult to provide because of the complexity of the processes. By publishing this PIA and subsequent updates, USCIS is attempting to mitigate this by setting out the processes in a clear manner. Additionally, the development and deployment of the centralized system will streamline the process and thus improve transparency of the processes.

Privacy Risk: There is also a risk that the CICS mobile fingerprint units may be lost or stolen.

Mitigation: USCIS has followed DHS and OMB guidelines for encrypting all CICS mobile devices to ensure the data cannot be compromised.

Privacy Risk: Adding the biometrics to the incorrect applicant file.

Mitigation: The information collected is attributed to the correct applicant file by matching fields such as A-Number Integrity checks are conducted at all points of data transfer and matching.

Section 2.0 Uses of the system and 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 biographical and biometric information collected at USCIS ASCs, refugee camps, and overseas offices and stored in and disseminated by FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest is used to complete the background checks required by USCIS. The results of the background checks are used to determine an applicant's eligibility for a USCIS benefit. If the background checks result from the FBI yields an item of law enforcement or national security interest, USCIS may work with CBP, the FBI, or other law enforcement entities, such as ICE, to determine if law enforcement actions should be pursued.

Additionally, the information in these systems may be used for future law enforcement action if that information, viewed in conjunction with other information not currently known, indicates that a crime may have been committed. If the applicant becomes the subject of a national security or law enforcement investigation, the information in these systems could be provided to law enforcement and the courts in the interest of public safety.

The information processed through BBSS is also used for card production.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as data mining)?

FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest are not used to analyze data in order to assist users in identifying previously unknown areas of note, concern, or pattern.

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

The information collected from applicants and entered into BBSS (via an electronic interface) and FMNS (via a manual process) is checked for accuracy. BBSS and FMNS have various validation tables, which are used to ensure the information and proper formatting prior to the transmission to the FBI. Data integrity checks are also performed to verify that the system is uploading the correct data. These checks match the A-Number, receipt number, first and last names, DOB, and other biographical information. If incorrect information is used to conduct a background check that results in the return of derogatory information for someone other than the applicant, the applicant has an opportunity during the adjudication

process to provide correct information and have the corrected information submitted to the agency conducting the check (e.g., FBI, US-VISIT/IDENT) for a new search.

In most cases, the refugee applicants in refugee camps have no identification documents when they are initially processed into CICS but if documentation such as a passport is available, then that is used to establish identity. Accuracy of biographic information is dependent on information provided by the refugee applicant. The USCIS Refugee Corps Officer types in the applicant's biographical information, takes a photo, and processes the fingerprints into the CICS application. CICS validates all demographic data to ensure that the data is compliant with the EFTS format defined by BBSS prior to sending a submission. The Refugee Asylum and International Operations (RAIO) Officers who review these documents have received training in fraud detection. Additionally, Fraud Detection Officers are assigned to most of the overseas offices.

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

Privacy Risk: Misuse of data.

Mitigation: FBI fingerprints and biometrics request and response records are attributed to the correct applicant file by matching fields such as A-Number, name, and DOB. Fingerprints themselves are biometrically verifiable. When a benefit is denied, the adjudicator must site the reason and section of law under which the denial was based. The applicant has the opportunity to appeal this decision. USCIS has standard operating procedures in place to instruct adjudicators on the review of RAP Sheets and how to conduct TECS Enforcement reviews. If a report is placed in the wrong file, the adjudicator may correct the misplacement and the applicant has the opportunity to correct during the interview.

Integrity checks are conducted at all points of data transfer and matching. All FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest information resides on and is connected to a secured network and servers with access limited to authorized personnel only. Audit logs are retained to track and identify unauthorized uses of system information. Information including the user's identity accessing the systems, time/date of access, and the events that occurred, sources of these events, and the outcomes of these events. If misuse of data is suspected, these logs can be used to review and analyze all activity in system. The misuse of data could be detected by reporting from employee and/or system monitoring. All FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest users are notified that these logs are stored and that USCIS management can use these to review any and all activity related to system usage.

Section 3.0 Retention

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

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

FMNS

Data in FMNS is only retained for 60 days.

CICS

No information is stored in CICS. The information is collected and transferred to BBSS or an encrypted portable storage device if network access is not available.

FD-258 MF

The biographic data and FBI response data contained in FD-258 MF is retained for 75 years pending National Archives and Records Administration (NARA) approval.[12]

BBSS

The biographic data and FBI response data, including RAP Sheets are retained indefinitely in BBSS per the requirements of the USCIS Office of Financial Operations (OFO) as approved by NARA.

IBIS Manifest

The biographic data and name check results are retained for 180 days. The results of the TECS Name Check are also placed in the A-File.

Paper Records Associated With Background Check Processes

The paper version of the RAP Sheet and TECS Name Check is maintained in the applicant's A-File for 100 years from DOB. The files are then turned over to NARA for permanent retention.

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

Retention schedules for FMNS [N1-566-08-2], FD-258 MF [N1-85-00-1], and BBSS [N1-566-08-3] have been approved by NARA. A retention schedule for IBIS Manifest is being drafted and will be submitted to NARA for approval.

[12] The current record published in the Federal Register states that the data in FD-258 is deleted 10 years after the last action. This retention timeframe is incorrect and an updated retention schedule is being submitted to the National Archives & Records Administration (NARA) and will be published in the Federal Register.

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

Privacy Risk: Keeping data longer than necessary would violate the Fair Information Practice that requires the retention of the minimum amount of information necessary to perform relevant governmental functions.

Mitigation: The information is needed for the indicated time period because the relationship between an applicant and USCIS may span the time period that the data is retained. USCIS will use the historical data in the systems for the adjudication of applications/petitions in the future. All data and electronic images are being retained for the indicated periods to fulfill the business requirements of DHS and in accordance to the limits of the retention schedules, which includes adjudication of 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. USCIS recognizes the indefinite retention of BBSS files is not consistent with retaining records for only as long as needed for agency business and as a result, once the new system which will consolidate the information goes live, the retention periods will change to 100 years from the DOB.

The ability to forge identities is a growing concern and keeping this biographic data on record for lengthy periods of time can help protect against fraudulent benefit applications. USCIS has implemented several measures to combat identity fraud and storing all background check data for future use supports this initiative.

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 organizations is the information shared?

FD-258 MF shares information internally with CLAIMS 4, RAPS, and CLAIMS 3.

BBSS shares information internally with the US-VISIT program's IDENT system through the interface for fingerprint/biometrics image purposes. BBSS also sends information to the FD-258 MF via FD-258 EE.

IBIS Manifest conducts queries against the CBP TECS system. A history action code is placed in CLAIMS 3 if there is no derogatory information.

In addition, USCIS may share background check information within DHS where background responses yield information that may indicate a violation of immigration, criminal, or terrorism-related laws. Specifically, USCIS may share with CBP, ICE, and Office of Intelligence & Analysis.

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

FMNS does not share data directly. The biographic information entered into FMNS is printed on the FD-258 card. The applicant's 10-prints are captured on that same card. The FD-258 cards are sent to one of the service centers where they are scanned into BBSS. An EFTS record is created and electronically sent to the FBI for the 10-print criminal background check.

FD-258 MF shares information internally with CLAIMS 4, RAPS, and CLAIMS 3 to facilitate the adjudication of immigration benefits.

After BBSS captures the 10-Prints, they are transmitted to IDENT with associated biographic information to match against the IDENT database. This search is required in order to complete the IDENT fingerprint background check. US-VISIT uses the information to enroll the applicant into IDENT so biometric identification and verification can be performed in future encounters.

IDENT stores all biometric and biographic data transmitted from BBSS. US-VISIT also shares this information with CBP and other DHS components if US-VISIT determines that the receiving component has a need to know to carry out national security, law enforcement, immigration, intelligence, and other DHS mission-related functions.

TECS Name Check requests and responses are shared electronically between IBIS Manifest and the TECS Name Check system. IBIS Manifest electronically sends the applicant's first and last name, DOB, gender, and unique subject ID (either receipt number or A-Number) to initiate a name check request. CBP uses this information to conduct a name check against the TECS Name Check system, and sends the results back to IBIS Manifest. A history action code is placed in CLAIMS 3 if there is no derogatory information. If a TECS Name Check result contains items of law enforcement interest and national security concerns, USCIS may provide the information to other law enforcement entities such as ICE to determine if further law enforcement activities should be pursued.

4.3 How is the information transmitted or disclosed?

FBI fingerprint/biometrics images are sent electronically to US-VISIT in an unencrypted format within the DHS firewall. Transactions between BBSS and the FBI are conducted using the required EFTS format through a secure and reliable electronic interface. All transmissions to and from the FBI are encrypted.

Paper-based transmissions of RAP Sheets from the FBI are sent to USCIS via secure DOJ mail carrier.

TECS Name Check requests and responses are sent electronically between IBIS Manifest and TECS Name Check system.

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

Privacy Risk: Unauthorized access.

Mitigation: Internal sharing of data is conducted over secured networks controlled by DHS utilizing DHS approved computers, services, and software. The privacy risks associated with each step of internal sharing, including system and network security, data usage, data transmission, and disclosure have been identified and mitigated through adherence to DHS policies and procedures such as Information Technology Lifecycle Management (ITLM) that includes System Design Life Cycle (SDLC) documentation and Certification and Accreditation (C&A) documentation. In addition, only authorized users who need the information collected and contained in FMNS, CICS, FD-258 MF, BBSS, or IBIS Manifest have access to the system.

Privacy Risk: Misuse of data.

Mitigation: Given the technical security aspects above, there will always be the possibility of misuse and inappropriate dissemination of information. To help mitigate these risks, security logs, audit logs of user activity, and strict access controls are enforced. FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest users are granted access to these systems only after requesting access through their manager and the appropriate System Administrator.

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 organizations is the information shared?

BBSS shares information with the FBI.

The information related to the UK Visa project outlined in the Introduction passes through BBSS and is sent to the UK government. It is deleted as soon as the data transfer is confirmed.

FMNS, CICS, FD-258, and IBIS Manifest do not share information with any organization outside of DHS.

Information resulting from the background check processes may be printed out and placed in the customer A-File. The A-File may be shared with external organizations such as immigration judges and other federal agencies. For a full discussion of the external sharing of the A-File, please see the A-File System of Records Notice (SORN), http://edocket.access.gpo.gov/2007/E7-375.htm.

5.2 What information is shared and for what purpose?

BBSS sends the EFTS 10-print record to the FBI to conduct a criminal background check against its IAFIS system.

As discussed in a separate PIA, BBSS also facilitates the transfer of biometric and biographic data pursuant to the UK Visa Program.

5.3 How is the information transmitted or disclosed?

FBI Fingerprint Check requests and responses are electronically transmitted through BBSS to and from the FBI's IAFIS system. FBI fingerprint and other biometric information and the responses are encrypted when electronically transmitted between BBSS and the FBI. The data exchange between USCIS and the FBI for the purpose of FBI Name Check occurs via zipped and encrypted email. For military applicants, if previous fingerprints are found, the liaison returns the fingerprint records on an encrypted compact disc to the Nebraska Service Center (NSC). Personnel at the NSC format these fingerprints from the compact disc and submit them through BBSS to the FBI for the required background check.

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

USCIS has an existing MOU with the FBI (cited above) and US-VISIT that sets forth the terms and conditions for the transfer and use of information pertaining to background checks. USCIS also has an existing ISA with the United Kingdom. *Interconnection Security Agreement between USCIS and UK BBSS and UK VISAS, November 16, 2007*.[13]

5.5 How is the shared information secured by the recipient?

The recipient of the shared information is the FBI. The information provided to the FBI by USCIS is restricted to FBI employees with Top Secret clearances who work in secure facilities. The information transmitted is stored in FBI information systems that have been certified and accredited by the FBI in accordance with DOJ and National Institute of Standards and Technology (NIST) requirements.

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

The external agency receiving access to the information sent by BBSS to the FBI IAFIS is the FBI. This information is used by FBI to perform criminal background check. The transfer of the data is

[13] USCIS is currently drafting an updated ISA for the UK VISAS Program.

conducted pursuant to the MOU between USCIS and the FBI. FBI employees who perform criminal background checks have received the required training to perform the checks.

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

Privacy Risk: Unauthorized access.

Mitigation: When BBSS sends information to and receives information from the FBI, the data is shared over DHS and FBI secured networks. FBI employees are trained and authorized to deal with biographic and biometric data. In addition, the FBI has policies and procedures in place to ensure that information is not inappropriately disseminated.

Privacy Risk: Misuse of data.

Mitigation: There is a possibility of misuse and inappropriate dissemination, but these risks are mitigated by taking advantage of the DHS Security specifications that require audit logs of user activity, security logs, and strict access controls. The risk associated with the fingerprint and biometric data that is transmitted to the FBI is also mitigated by the encryption of this data in accordance with DHS and NIST guidelines.

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

The information in FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest are covered by DHS/USCIS SORN - 002(72 FR 31082), *Background Check Service*[14] and DHS/USCIS SORN - 003(72 FR 17172), *Biometric Storage System*.[15] This notice provides individuals with notice prior to the collection of information. Notice of also provided on all USCIS forms at the point of collection. (See Section 6.2).

[14] Available at http://edocket.access.gpo.gov/2007/07-2782.htm.
[15] Available at http://edocket.access.gpo.gov/2007/07-1643.htm.

6.2 Do individuals have an 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.

USCIS benefit applications require that certain biographic information be provided and may also require submission of fingerprints and photographs. This information is critical in making an informed adjudication decision in granting or denying a USCIS benefit. The failure to submit such information would prohibit USCIS from processing and properly adjudicating the application/petition and thus preclude the applicant from receiving the benefit. Therefore, through the application process, individuals have consented to the use of the information for adjudication purposes, including background investigations.

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

Individuals who apply for USCIS benefits are presented with a Privacy Act Statement as required by Section (e)(3) of the Privacy Act and sign a release authorization on the benefit application/petition. The Privacy Act Statement details the authority to collect the information requested. The forms also contain a provision by which an applicant authorizes USCIS to release any information received from the applicant as needed to determine eligibility for benefits.

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

Privacy Risk: The privacy risk associated with this particular collection of information is that the individual may not be fully aware that their information will be used to conduct an inquiry into benefits eligibility.

Mitigation: The collection of PII is a required part of the adjudication process, which must occur prior to the granting of an immigration benefit. The privacy risk associated with this particular collection of information is that the individual may not fully understand how the data will be used to conduct background checks. In order to mitigate this risk, USCIS has provided a Privacy Act Statement on all benefit application/petition forms. The form also contains a signature certification and authorization to release any information provided by an applicant. The information in FMNS, CICS, FD-258 MF, BBSS,

and IBIS Manifest is covered by DHS/USCIS SORN - 002 (72 FR 31082), *Background Check Service* and DHS/USCIS SORN - 003(72 FR 17172), *Biometric Storage System.* The publication of the SORNs and this PIA serve as additional notice to individuals regarding the use of the information in all five systems.

Section 7.0 Individual 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 which allow individuals to gain access to their own information?

USCIS treats all requests for amendment of information in a system of records as Privacy Act amendment requests. Any individual seeking to access information maintained in these systems should direct his or her request to the USCIS FOIA/Privacy Act (PA) Officer at USCIS FOIA/PA, 70 Kimball Avenue, South Burlington, Vermont 05403-6813 (Human resources and procurement records) or USCIS National Records Center (NRC), P. O. Box 648010, Lee's Summit, MO 64064-8010 (all other USCIS records). The process for requesting records can be found at 6 Code of Federal Regulations (C.F.R.) § 5.21.

Requests for access to records in this system must be in writing. Such requests may be submitted by mail or in person. If a request for access is made by mail, the envelope and letter must be clearly marked "Privacy Access Request" to ensure proper and expeditious processing. The requester should provide his or her full name, date and place of birth, and verification of identity (full name, current address, and date and place of birth) in accordance with DHS regulations governing Privacy Act requests (found at 6 C.F.R. § 5.21), and any other identifying information that may be of assistance in locating the record.

The information requested may, however, be exempt from disclosure under the Privacy Act because FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest files with respect to an individual may sometimes contain law enforcement sensitive information the release of which could possibly compromise ongoing criminal investigations.

If an individual would like to file a Privacy Act request to view their USCIS record the request can be mailed to the following address:

National Records Center
Freedom of Information Act/Privacy Act Program
P. O. Box 648010,
Lee's Summit, MO 64064-8010

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

7.2 What are the procedures for correcting erroneous information?

In addition to the Privacy Act procedure discussed above, if an individual determines that information in FMNS, CICS, FD-258, BBSS, or IBIS Manifest is inaccurate during the application and adjudication process, the individual can file a USCIS form for a name change located on the USCIS website, directed at changing the specific erroneous information.[16] For information such as an incorrect A-Number, the individual may contact USCIS' customer service number at 1-800-375-5283 (TTY 1-800-767-1833) to make the correction. USCIS personnel submit a ticket to the USCIS Help Desk requesting that the erroneous information be corrected. The correct information is then provided by the applicant and verified (if necessary). The Help Desk forwards the request to an authorized system administrator and the erroneous information is corrected. If an applicant believes their file is incorrect, but does not know which information is erroneous, the applicant may file a Privacy Act request as detailed in Section 7.1.

If the particular USCIS process requires a personal interview by a USCIS examiner in order to adjudicate a benefit application, the applicant also has the opportunity to request changes to correct erroneous information during the interview.

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

Individuals are notified of the procedures for correcting their information on USCIS forms, in the SORNs and PIA covering the information in these systems, and by USCIS personnel who interact with benefit applicants.

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

USCIS provides redress to applicants as outlined in Sections 7.1 and 7.2.

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

Privacy Risk: The main risk with respect to redress is that the right may be limited by Privacy Act exemptions or limited avenues for seeking redress.

Mitigation: The redress and access measures offered by USCIS are appropriate given the purpose of the systems. Individuals are given numerous opportunities during and after the completion of

[16] The USCIS website contains links to all available USCIS forms. These forms include the AR-11 address change form as well as other immigration forms which may be used to amend information located in the individual's record.

the applications process to correct information they have provided and to respond to information received from other sources including receiving information about why a benefit was denied and their appeal rights.

Privacy Risk: There is a risk that a FOIA or Privacy Act request may not be expansive enough to include a search of specific systems or the records search may only include the A-File.

Mitigation: To mitigate this risk, USCIS places a hard copy of the RAP Sheet (if applicable) and results from the FBI Name Check (if positive) in the applicant's A-File which ensures that the requestor gains access to the information when appropriate under the FOIA and Privacy Act.

Section 8.0Technical Access and Security

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

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

USCIS deploys role-based access controls to limit access to only those persons who have a need to know this information in order to perform their duties. In compliance with federal law and regulations, users have access to FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest on a need to know basis. This need to know is determined by the individual's current job functions. Users may have read-only access to the information if they have a legitimate need to know as validated by their supervisor and the system owner and have successfully completed all personnel security training requirements. System administrators may have access if they are cleared and have legitimate job functions that would require them to view the information. Developers do not have access to production data except for specially cleared individuals who perform systems data maintenance and reporting tasks. Access privileges are limited by establishing role-based user accounts to minimize access to information that is not needed to perform essential job functions.

A user desiring access must complete a Form G-872A & B, USCIS and End User Application. This application requires justification for the level of access being requested. The requestor's supervisor, the system owner, and the USCIS Office of the Chief Information Officer (OCIO) review this request; if approved, the requestor's clearance level is independently confirmed and the user account is established.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Contractors are used to maintain systems and to provide technical support. Access is provided to contractors only as needed to perform their duties as required in the agreement between USCIS and the contractor and as limited by relevant USCIS and DHS policies. In addition, USCIS employees and contractors who have completed a G-872A & B form (See Section 8.1) and granted appropriate access

levels by a supervisor are assigned a login and password to access the system. These users must undergo federally approved clearance investigations and sign appropriate documentation in order to obtain the appropriate access levels. All access to the FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest systems follow the logical access controls set up for access to USCIS computer systems. Access controls are applied to contractors and to federal employees equally.

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

There are two classes of users for FMNS:

- Class 1 – Read/Write/Query – Users that enter masthead data, generate manifests and generate fingerprints appointment notices and have query capabilities; and
- Class 2 – System Administrator – Users requiring system administrative privileges.

There are two classes of users for CICS:

- Class 1 – RAIO Officer – captures and processes applicant biographic and biometric data; and
- Class 2 – Application Administrator – has the ability to modify configuration settings for the CICS application

There are two classes of users for FD-258:

- Class 1 – Query – Read access only. Users can query by A-Number or Name and DOB; and
- Class 2 – System Administrator – Users requiring system administrative privileges.

There are four classes of users for BBSS:

- Class 1 – User – Users requiring Fingerprint and Biometrics submission and query capabilities;
- Class 2 – Power User – Users requiring Fingerprint and Biometrics submission;
- Class 3 – Administrator – Users requiring all standard functions and the ability to run reports; and
- Class 4 – System Administrator – Users requiring system administrative and database administrative privileges. This class is reserved for authorized contractors that support BBSS who are located at the USCIS HQ location. Moreover, this class is not assigned to any user located at a USCIS field site.

There two classes of users for IBIS Manifest:

- Class 1 – Query – Read access only; and
- Class 2 – System Administrator – Users requiring system administrative privileges.

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

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

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

To ensure that users do not use the data outside of scope of their official job duties, audit trails are kept to track and record the activity of each user. Reports can also be run against each system to verify that a user's activity is consistent with his or her permissions.

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

FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest maintain audit logs on all transactions and user activities. Because Fingerprint/Biometrics data requests can be resubmitted based on poor or problematic images, audit trails are required to ensure that the Fingerprint/Biometrics data requests are not duplicated. Therefore, BBSS also provides audit trail records that record efforts to resubmit, review, and examine the originally submitted FBI Fingerprint/Biometrics request transactions. All transactions are subject to monitoring and review to ensure that the original requests or results are not lost, manipulated, or compromised in any manner. Lastly, NIST approved data encryption is used for data transportation between USCIS and the FBI to ensure that data has not been tampered with en-route and to prevent unauthorized personnel from accessing the data.

Locally employed staff at USCIS overseas field offices who are not US Citizens must have a DHS systems waiver to operate the CICS fingerprint units.

USCIS has followed DHS guidelines for encrypting all CICS mobile devices to ensure the data cannot be compromised. In addition, USCIS employs two-factor authentication for the fingerprint devices. CICS will comply with physical and logical security policies applicable to systems within the USCIS enterprise. This requires the protection of applicant data during capture through transmission to backend USCIS systems, secure transmission of sensitive data through the use of digital certificates and Secure Socket Layer (SSL) transactions, and username and password required for system access.

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

USCIS provides training to all FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest users. This training addresses appropriate privacy concerns, including Privacy Act obligations (e.g., SORN, Privacy

Act Statements, etc.). Each USCIS site has the responsibility to ensure that all federal employees, locally employed staff, and contractors receive the required annual security and Privacy Act training.

In addition, USCIS employees, locally employed staff, and contractors who have completed a G-872B form (See Section 8.4) and have been granted appropriate access levels (See Section 8.3) by a superior are assigned a login and password from the appropriate System Administrator used to access the system. These users have previously undergone federally approved clearance investigations and signed appropriate documentation in order to obtain the appropriate access levels.

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

The fingerprint/biometrics data that is captured, processed, and stored by FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest is secured in accordance with Federal Information Security Management Act (FISMA) requirements. The authority to operate (ATO) for BBSS was issued on June 29, 2009 and expires on June 29, 2012. FMNS is a subsystem under BBSS and follows the BBSS ATO. CICS also falls under the BBSS ATO. FD-258 MF was certified and accredited on July 31, 2008 for a three year period expiring July 31 2011. IBIS Manifest is covered under the CISCOR C&A. The ATO for CISCOR, which includes IBIS Manifest, was issued on March 21, 2008 and expires on March 28, 2011.

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

Privacy Risk: Due to the sensitive nature of this information, there are inherent security risks (e.g., unauthorized access, use and transmission/sharing) that require mitigation.

Mitigation: Access and security controls have been established to mitigate privacy risks associated with authorized and unauthorized users, namely misuse and inappropriate dissemination of data. Authorized users are broken into specific classes with specific access rights. Audit trails are kept in order to track and identify unauthorized uses of system information. Data encryption is employed at every appropriate step to ensure that only those authorized to view the data may do so and that the data has not been compromised while in transit. Since FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest have been implemented in the production environment, authorized users are organized into specific classes with specific access rights, audit trails are retained to track and identify unauthorized uses, and data encryption is employed at every appropriate point to verify that only authorized users can view the data and the data is not compromised during transmission. Further, FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest comply with the DHS security guidelines, which provide hardening criteria for securing networks, computers and computer services against attack, and unauthorized information dissemination.

CICS will be developed with security provisions intended to prohibit unauthorized access and modification to system resources. Such provisions include installation on approved USCIS computing

resources, to include use of encrypted hard drives for laptop deployments.

CICS will enable RAIO Officers to upload applicant information to a centralized USCIS system, which is currently BBSS. The information can only be uploaded when secure communications with the USCIS network is established. In the event that communications with the USCIS network is not possible, CICS will enable RAIO Officers to save applicant information to secured portable media for manual processing.

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

The FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest systems were designed and implemented with both commercial off-the-shelf products and custom designed software, databases, and user interfaces.

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

FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest developers followed the ITLM and SDLC security guidelines in the design and development of FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest respectively. All documentation has been reviewed and approved by USCIS OIT IT Security. Background check requests and result records are attributed to the correct applicant file by matching multiple data points including A-Number, receipt number, last name, and DOB.

9.3 What design choices were made to enhance privacy?

FMNS, CICS, FD-258 MF, BBSS, and IBIS Manifest are only available to USCIS employees and contractors who have appropriate security and access controls. The general public does not have access to these systems. Protection and integrity of data, security, and privacy are of paramount concern. These systems follow all DHS Security guidelines for enhanced security including the C&A security documents, Federal Information Processing Standards 199, FISMA, Trusted Agent - FISMA, OMB memoranda, and NIST security guidelines.

Responsible Officials

Donald Hawkins
USCIS Privacy Officer
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