



**Homeland  
Security**

**JUL 29 2004**

The Honorable Jim Turner  
U.S. House of Representatives  
Washington, DC 20515-3808

Dear Representative Turner:

On behalf of Secretary Ridge, thank you for your letter regarding the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program. The Department of Homeland Security values your interest in this program and appreciates this opportunity to respond to your biometrics survey. The Department has completed the survey from each of the DHS bureaus and is forwarding it to Jessica Herrera of your Committee as requested.

I appreciate your interest in the Department of Homeland Security, and I look forward to working with you on future homeland security issues. If I may be of further assistance, please contact the Office of Legislative Affairs at (202) 205-4412.

Sincerely,

A handwritten signature in cursive script that reads "Pamela J. Turner".

Pamela J. Turner  
Assistant Secretary for Legislative Affairs

Enclosure

## Summary: Department of Homeland Security Biometrics Survey

A summary of DHS' biometrics programs and initiatives follows; detailed survey responses, Privacy Impact Assessments, and relevant policies and procedures are provided as Attachments.

### **Does your agency currently collect, or plan to collect in the future, biometrics from the general public for any of its programs and initiatives?**

DHS collects biometrics from the 'general public' for the purposes of conducting background checks, freezing identity, searching watch lists, reducing fraud, and improving border and transportation and maritime security.

### **Please identify the program/initiative and the purpose for using biometrics.**

1. In support of Border and Transportation Security (BTS) initiatives, the following programs collect biometrics for identity verification against previously enrolled biometric information, searching terrorist watch lists, and/or conducting background checks to identify criminals or previously deported persons.
  - U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) uses biometrics to verify the identity of aliens applying for entry to the United States against previously enrolled biometric data.
  - Customs and Border Protection (CBP) collects biometrics for expedited inspections at the southern and northern land borders through: the NEXUS Highway, a northern land border partnership with Canada under the Shared Border Accord, captures two index fingerprints for identity verification; the Free and Secure Trade Program (FAST) collects biometrics to use in background checks for a driver identification RFID card; and, Secure Electronic Network for Travelers Rapid Inspection (SENTRI) captures biometrics to conduct background checks on applicants for its dedicated commuter lane program. CBP also plans to collect and verify biometrics for expedited processing of pedestrians. Additionally, the Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS) collects biometrics to validate the claimed identity of pre-enrolled travelers.
  - The Transportation Security Administration (TSA) plans to collect biometrics for two programs. In May 2004, the Transportation Worker Identity Credential (TWIC) system will collect biometrics for transportation workers who require access to secure areas of the nation's transportation system. The Registered Traveler (RT) and Armed Law Enforcement Officer (LEO) pilot, scheduled for June 2004, will use biometrics for background screening of frequent fliers and to identify Federal law enforcement officers.
2. The U.S. Bureau of Citizenship and Immigration Service (USCIS) collects biometrics from persons applying for a variety of citizenship and immigration benefits. Biometrics are used to conduct criminal background checks and to produce documents issued by USCIS, such as Permanent Resident Cards (PRCs).

3. The U.S. Coast Guard (USCG) collects biometrics for the Department of Justice Criminal History Check for all License and Merchant Marine Document (MMD) applications and renewals.

**What is the type of biometrics technology used?**

All of the programs except INSPASS use fingerprint matching. INSPASS uses hand geometry biometric image technology. The US-VISIT, SENTRI, NEXUS, FAST, USCIS, and TWIC programs also collect facial photographs. The photographs taken at document issuance for the BTS programs are used as a secondary identity verification tool at the port of entry. In the future, visa waiver travelers holding chip-enabled passports will have their identity verified using facial recognition. TSA plans to also use iris recognition in addition to fingerprint matching for the TWIC and RT/Armed LEO pilot programs. USCIS incorporates photographs and a fingerprint into cards and travel documents. The USCG currently uses the FD258 Standard Finger Print Card to capture biometrics.

**How much did it cost your agency to implement the use of biometrics for the program/initiative and what is the FY04 projected cost for using the technology?**

Implementation costs for the US-VISIT and USCIS programs total \$260M. The FY04 budget for these programs is \$148M. The FAST program costs are currently estimated at \$417,922 with any additional costs dependent upon the number of driver cards issued. The estimated FY04 cost for INSPASS is \$1.7 million. The SENTRI pedestrian test and TWIC system have incurred no expenditures to date; the FY04 budget to implement the RT and Armed LEO pilot is \$5M. The USCG FD258 Standard Finger Print Card costs \$18 per card with an estimated \$620,000 budgeted for fingerprint card processing (estimate does not include civil service or contractor salary).

**Is the use of biometrics for this program or initiative mandated by statute or rule? If so, please explain how, or provide the statutory or regulatory citation.**

Use of biometrics for US-VISIT is mandated by the Enhanced Border Security Act; for TWIC, the mandates are contained in the Maritime Transportation Security Act and the Aviation and Transportation Security Act; the use of biometrics for USCIS is based on multiple statutory and regulatory mandates, including Title 8 of the U.S. Code, 8 CFR, and Public Law 105-277. The Coast Guard initiatives result from 46CFR10.201(h) (1-6) Criminal Record Review for all Licenses, 46CFR12.02-4(c) (1-6) Criminal Record Review for Certification (MMD), and Commandant Instruction M16000.8B Marine Safety Manual; Volume III Marine Industrial Personnel; Chapter 8 Record Management for U.S. Merchant Mariners; A. Records Management; 10-Preparation of Fingerprint Records.

**How is the biometrics information gathered, collected, and stored?**

For US-VISIT, a photograph and fingerprints are captured from a visa applicant at a consular post and stored in a Department of State (DOS) database. Fingerprints are forwarded to the US-VISIT database for searching; the prints and relevant biographic information are also stored in the US-VISIT database. At the port of entry, the inspector

retrieves the photograph from the DOS system and compares it to the traveler; the traveler's fingerprint is collected via a fingerprint scanner and verified against the print taken at visa application.

Biometric information is collected during the enrollment process for FAST, NEXUS, INSPASS and SENTRI, at their respective enrollment centers. The FAST digital photographs are stored electronically ; fingerprints are forwarded to the FBI and are not stored in DHS systems. The fingerprints collected for the NEXUS program are stored in the Automated Biometric Identification System (IDENT). Biometric data for INSPASS is stored in the Treasury Enforcement Communications System (TECS).

TSA collects biometric information during the TWIC enrollment process; the biometric images are stored in a segmented database and on a smartcard. For the RT pilot, biometrics will be gathered during enrollment, and stored on a smartcard or other token as well as in a database.

USCIS collects biometrics from applicants for immigration benefits at Application Support Centers. Fingerprint images are retained on tapes and not readily accessible; transaction and biographic data is stored in a fingerprint tracking system. Biometrics used to construct documents and travel cards are stored in USCIS' view-only Image Storage and Retrieval System (ISRS).

The Coast Guard fingerprints (and duplicate) are collected at 17 Regional Exam Centers (REC); sent to the National Maritime Center (NMC) and forwarded to the Federal Bureau of Investigation (FBI). Duplicate Fingerprint Cards are kept on file at NMC in a locked cabinet and destroyed after two years.

**Is the information accessible by other agencies or other entities (including contractors, vendors, and state and local governments)?**

Contractor access to US-VISIT information is limited to that necessary for system maintenance and development; US-VISIT has agreements with the FBI for the exchange of information on terrorists and other persons of interest. Information may be supplied to law enforcement agencies in response to specific inquiries.

For FAST the photos and fingerprints are sent to the Canadian Border Service Agency (CBSA) and the Royal Canadian Mounted Police (RCMP). NEXUS information could be accessed by anyone who has access to the IDENT system; the Department of Justice/FBI has access to IDENT. The SENTRI Pedestrian information will be accessible to contractors responsible for system installation. INSPASS information is accessible by the contractor.

Information collected for the TWIC program is not accessible to other agencies, but will be submitted to other agencies for background investigations. Information gathered for the RT and Armed LEO pilots will be accessible by agencies in response to queries regarding risks to transportation or national security; air piracy or terrorism; or aviation

safety. RT information will also be accessible to the General Services Administration and the National Archives and Records Administration for records management inspections.

USCIS biometric data is accessible to the FBI for background checks; to US-VISIT for identity verification; and to contractors who support USCIS benefits systems.

USCG information is available if requested, but no requests have been received to date.

**Please describe the security measures used to protect the biometric information that is gathered, including any limitations on accessing the information.**

Access to US-VISIT information is on a password control basis and each transaction is logged. SENTRI pedestrian data is protected in accordance with DHS security policy. For FAST information will be compliant to security measures as outlined by current OIT policy. Information in NEXUS is secured via the IDENT system. INSPASS hand geometry templates are stored in a repository for all users of the system and protected by the Privacy Act.

Security measures for the TWIC program include recording transactions, automatic deletion of data from workstations, and encryption of all data in transmission and storage. Fingerprint images are stored in segmented databases to dissociate the image from the personal information; biometrics stored on smartcards are encrypted. Access to personal data in the TWIC system will be granted only to appropriate authorities; access privileges will be secured using biometrics. Biometrics information for the RT pilot will be secured in accordance with TSA and DHS security and access policies; system access will follow the least privilege principle.

Access to the USCIS ISRS system is controlled by passwords; transactions are logged. For the USCG DOJ criminal reports are mailed to the local REC. Fingerprint cards and criminal reports at NMC are kept in a locked cabinet until mailed or destroyed.

**Did your agency conduct any privacy assessments for this use of biometrics?**

See Attachments 1B, US-VISIT Privacy Impact Assessment (PIA), and 7A, USCIS PIA. A PIA was not conducted for FAST, INSPASS or the SENTRI Pedestrian test (NEXUS "unknown"). A draft PIA has been developed for TWIC, and a PIA is in process for the RT Pilot program. No privacy impact assessment was done for the USCG. Merchant Marine Fingerprints have been taken by the Coast Guard since 1936, prior to the Privacy Act of 1974.

**At what rate have false-positives been returned during the use of biometrics in this program?**

For US-VISIT, fingerprints captured at visa application are searched against databases of inadmissible persons; if a potential match is found, it is checked by a biometrics professional before making a final determination. At the port of entry, the traveler's

fingerprints are collected and compared to the traveler's enrolled data; in combination with document examination and an interview, false positives are nearly impossible.

Since the TWIC and RT have not yet begun, there is no data available. USCIS has noted no instances of false positives; neither has the INSPASS program. For NEXUS and the USCG the currently available data is insufficient to generate an accurate measurement of false positives.

**What is the process in place to ensure that there is not repeated false-positives in the system?**

Because of the additional document and interview checks conducted for US-VISIT, this does not apply. Processes will be developed as needed based on results from the TWIC and RT pilot programs. USCIS has not experienced false positives; therefore a process is not applicable.

**Please provide a copy of any procedures or policies your agency has in place regarding the use of biometrics. If these procedures or policies are program or initiative specific, please indicate so.**

DHS has established the Biometrics Coordination Group (BCG), co-chaired by a representative from US-VISIT and from the Office of Science and Technology. This group is chartered with developing policies for biometrics on a department-wide basis and reviewing development of new biometric projects. Its first task has been to develop the Policy on Facial Photographs, which is based on work of the International Standards Organization in facial recognition. Once this policy has been formalized, the BCG will address fingerprint and other biometric standards for the department.

Please see Attachment 1C, DHS US-VISIT Interim Standard Operating Procedures for Biometric Enrollment. Please reference each individual attachment for specific procedures and/or policies relating to individual programs or initiatives.

**Agency:** Department of Homeland Security  
**Contact:** b(6)  
**Telephone:** b(2), b(6)  
**E-mail:** b(2), b(6)@dhs.gov

## **LIST OF ATTACHMENTS**

**Attachment 1 – DHS Biometrics Survey: US-VISIT**

**Attachment 1A – DHS US-VISIT Pertinent Areas of Enhanced Border Security Act**

**Attachment 1B – DHS US-VISIT Privacy Impact Assessment**

**Attachment 1C – DHS US-VISIT Interim Standard Operating Procedures for Biometric Enrollment**

**Attachment 2 – DHS Biometrics Survey: SENTRI Pedestrian Test**

**Attachment 3 – DHS Biometrics Survey: TSA TWIC**

**Attachment 4 – DHS Biometrics Survey: TSA RT and Armed LEO Pilot**

**Attachment 5 – DHS Biometrics Survey: USCIS**

**Attachment 5A – USCIS Privacy Impact Assessment**

**Attachment 6 – DHS Biometrics Survey: US Coast Guard**

**Attachment 7 – DHS Biometrics Survey: CBP FAST**

**Attachment 8 – DHS Biometrics Survey: CBP NEXUS**

**Attachment 9 – DHS Biometrics Survey: CBP IDENT/IAFIS**

**Attachment 10 – DHS Biometrics Survey: CBP INSPASS**

**Attachment 1**  
**DHS Biometrics Survey: US-VISIT**

The DHS collects biometrics from the general public in the course of inspection at a port of entry as part of the **US-VISIT Program**. The following responses pertain to that program.

**Please identify the program/initiative and the purpose for using biometrics**

Biometric samples are used to verify the identity of aliens applying for entry to the United States. The biometric collected at the port of entry is compared to that collected by the Department of State at the time that the visa is issued. The biometrics captured at the port are also compared to a watch list of persons wanted by law enforcement agencies or previously deported from the U.S.

**What is the type of biometrics technology used?**

Fingerprints form the basis of identity verification processes in US-VISIT. A photograph is also captured as a secondary identity verification tool for aliens holding visas. Visa waiver travelers holding chip-enabled passports will have their identity verified against the ICAO-compliant information contained on the chip, which supports facial recognition.

**How much did it cost your agency to implement the use of biometrics for the program/initiative and what is the FY04 projected cost for using the technology?**

The FY04 budget supporting biometrics is approximately \$58M; amount required for maintenance of the US-VISIT program that was implemented with FY03 funds (\$140M).

**Is the use of biometrics for this program or initiative mandated by statute or rule? If YES, reference the statutory or regulatory citation.**

The Enhanced Border Security Act mandated the use of biometrics in the inspection process. See Attachment 1A.

**How is the biometrics information gathered, collected, and stored?**

The visa applicant provides a photograph and has fingerprints taken at a consular post. The Department of State (DOS) stores that data in their database system. The fingerprints are electronically forwarded to the US-VISIT fingerprint database (IDENT) for a check to determine if there is known adverse information associated with that person. The fingerprints are stored in IDENT with relevant biographical information at that time. The DOS then makes a determination as to grant a visa based upon this and other available information. If the visa is granted, at the time that the traveler applies for admission at a port of entry, the photograph from the DOS database is available to the inspector and the fingerprint is verified against that taken at the time of visa application.

**Is the information accessible by other agencies or other entities (including contractors, vendors, and state and local governments)?**

The US-VISIT Program has instituted strict controls over access to the information in its databases. Support contractors have access to the database information only to support system maintenance and development. For specific inquiries, records may be made available to state and local law enforcement agencies. The FBI and US-VISIT have established data exchange mechanisms to ensure that relevant information on terrorists and other persons of interest to the U.S. is accurately reflected in their databases.

**Please describe the security measures used to protect the biometric information that is gathered, including any limitations on accessing the information.**

Access to the IDENT system is on a password-control basis only. Each transaction is logged and auditable.

**Did your agency conduct any privacy assessments for this use of biometrics? If so, please attach copies of any relevant assessments.**

See the attached US-VISIT Privacy Impact Assessment (Attachment 1B)

**At what rate have false-positives been returned during the use of biometrics in this program?**

Fingerprints are captured at the time of visa application and compared to a database in order to determine if there is any existing adverse information associated with that individual. Professionals examine the fingerprints of potential record matches before any final determination is made.

At the time of application for entry to the US at a port of entry, the fingerprints are compared on a one-to-one basis to establish that the traveler is the person who was granted the visa. False positives (i.e. a traveler's fingerprint matching that of the visa applicant's) are almost impossible, especially given the added security aspects of the inspection process, including document examination and interview.

**What is the process in place to ensure that there is not repeated false-positives in the system?**

As mentioned above, this does not apply to US-VISIT due to the way it has been established.

**Attachment 1A**  
**Pertinent Sections of the Enhanced Border Security Act**

SEC. <<NOTE: Deadlines. 8 USC 1732.>> 303. MACHINE-READABLE, TAMPER-RESISTANT ENTRY AND EXIT DOCUMENTS.

(a) Report.--

(1) In general.--Not later than 180 days after the date of enactment of this Act, the Attorney General, the Secretary of State, and the National Institute of Standards and Technology (NIST), acting jointly, shall submit to the appropriate committees of Congress a comprehensive report assessing the actions that will be necessary, and the considerations to be taken into account, to achieve fully, not later than October 26, 2004--

(A) implementation of the requirements of subsections (b) and (c); and

(B) deployment of the equipment and software to allow biometric comparison and authentication of the documents described in subsections (b) and (c).

(2) Estimates.--In addition to the assessment required by paragraph (1), the report required by that paragraph shall include an estimate of the costs to be incurred, and the personnel, man-hours, and other support required, by the Department of Justice, the Department of State, and NIST to achieve the objectives of subparagraphs (A) and (B) of paragraph (1).

(b) Requirements.--

(1) In general.--Not later than October 26, 2004, the Attorney General and the Secretary of State shall issue to aliens only machine-readable, tamper-resistant visas and other travel and entry documents that use biometric <<NOTE: Standards.>> identifiers. The Attorney General

and the Secretary of State shall jointly establish document authentication standards and biometric identifiers standards to be employed on such visas and other travel and entry documents from among those biometric identifiers recognized by domestic and international standards organizations.

(2) Readers and scanners at ports of entry.--

(A) In general.--Not later than October 26, 2004, the Attorney General, in consultation with the Secretary of State, shall install at all ports of entry of the United States equipment and software to allow biometric comparison and authentication of all United States visas and other travel and entry documents issued to aliens, and passports issued pursuant to subsection (c)(1).

(B) Use of readers and scanners.--The Attorney General, in consultation with the Secretary of State, shall utilize biometric data readers and scanners that--

(i) domestic and international standards organizations determine to be highly accurate when used to verify identity;

(ii) can read the biometric identifiers utilized under subsections (b)(1) and (c)(1); and

[[Page 116 STAT. 554]]

(iii) can authenticate the document presented to verify identity.

(3) Use of technology standard.--The systems employed to implement paragraphs (1) and (2) shall utilize the technology standard established pursuant to section 403(c) of the USA PATRIOT Act, as amended by section 201(c)(5) and 202(a)(4)(B).

(c) Technology Standard for Visa Waiver Participants.--

(1) Certification requirement.--Not later than October 26,

2004, the government of each country that is designated to participate in the visa waiver program established under section 217 of the Immigration and Nationality Act shall certify, as a condition for designation or continuation of that designation, that it has a program to issue to its nationals machine-readable passports that are tamper-resistant and incorporate biometric and document authentication identifiers that comply with applicable biometric and document identifying standards established by the International Civil Aviation Organization. This paragraph shall not be construed to rescind the requirement of section 217(a)(3) of the Immigration and Nationality Act.

(2) Use of technology standard.--On and after October 26, 2004, any alien applying for admission under the visa waiver program under section 217 of the Immigration and Nationality Act shall present a passport that meets the requirements of paragraph (1) unless the alien's passport was issued prior to that date.

(d) Authorization of Appropriations.--There are authorized to be appropriated such sums as may be necessary to carry out this section, including reimbursement to international and domestic standards organizations.

#### SEC. 307. DESIGNATION OF PROGRAM COUNTRIES UNDER THE VISA WAIVER PROGRAM.

(a) Reporting Passport Thefts.--Section 217 of the Immigration and Nationality Act (8 U.S.C. 1187) is amended--

(1) by adding at the end of subsection (c)(2) the following new subparagraph:

“(D) Reporting passport thefts.--The government of the country certifies that it reports to the United

States Government on a timely basis the theft of blank passports issued by that country."; and

(2) in subsection (c)(5)(A)(i), by striking "5 years" and inserting "2 years"; and

(3) by adding at the end of subsection (f) the following new paragraph:

"(5) Failure to report passport thefts.--If the Attorney General and the Secretary of State jointly determine that the program country is not reporting the theft of blank passports, as required by subsection (c)(2)(D), the Attorney General shall terminate the designation of the country as a program country."

(b) Check <<NOTE: 8 USC 1736.>> of Lookout Databases.--Prior to the admission of an alien under the visa waiver program established under section 217 of the Immigration and Nationality Act (8 U.S.C. 1187), the Immigration and Naturalization Service shall determine that the applicant for admission does not appear in any of the appropriate lookout databases available to immigration inspectors at the time the alien seeks admission to the United States.

#### SEC. 308. <<NOTE: 8 USC 1737.>> TRACKING SYSTEM FOR STOLEN PASSPORTS.

(a) Entering Stolen Passport Identification Numbers in the Interoperable Data System.--

(1) In <<NOTE: Deadline.>> general.--Beginning with implementation under section 202 of the law enforcement and intelligence data system, not later than 72 hours after receiving notification of the loss or theft of a United States or foreign passport, the Attorney General and the Secretary of State, as appropriate, shall enter into such system the corresponding identification number for the lost or stolen passport.

(2) Entry of information on previously lost or stolen passports.--To the extent practicable, the Attorney General, in consultation with the Secretary of State, shall enter into such system the corresponding identification numbers for the United States and foreign passports lost or stolen prior to the implementation of such system.

(b) Transition Period.--Until such time as the law enforcement and intelligence data system described in section 202 is fully implemented, the Attorney General shall enter the data described in subsection (a) into an existing data system being used to determine the admissibility or deportability of aliens.

SEC. 603. <<NOTE: 8 USC 1772.>> INTERNATIONAL COOPERATION.

(a) International Electronic Data System.--The Secretary of State and the Commissioner of Immigration and Naturalization, in consultation with the Assistant to the President for Homeland Security, shall jointly conduct a study of the alternative approaches (including the costs of, and procedures necessary for, each alternative approach) for encouraging or requiring Canada, Mexico, and countries treated as visa waiver program countries under section 217 of the Immigration and Nationality Act to develop an intergovernmental network of interoperable electronic data systems that--

(1) facilitates real-time access to that country's law enforcement and intelligence information that is needed by the Department of State and the Immigration and Naturalization Service to screen visa applicants and applicants for admission into the United States to identify aliens who are inadmissible or deportable under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.);

(2) is interoperable with the electronic data system implemented under section 202; and

(3) performs in accordance with implementation of the technology standard referred to in section 202(a).

(b) Report.--Not <<NOTE: Deadline.>> later than 1 year after the date of enactment of this Act, the Secretary of State and the Attorney General shall submit to the appropriate committees of Congress a report setting forth the findings of the study conducted under subsection (a).

**Attachment 1B  
US-VISIT Privacy Impact Assessment**

**(Separate \*.PDF File)**



# **US-VISIT Program, Increment 1 Privacy Impact Assessment**

**December 18, 2003**

## **Contact Point**

**Steve Yonkers  
US-VISIT Privacy Officer  
Department of Homeland Security**

**(b)(2), (b)(6)**

## **Reviewing Official**

**Nuala O'Connor Kelly  
Chief Privacy Officer  
Department of Homeland Security**

**(b)(2), (b)(6)**

# US-VISIT Program, Increment 1

## Privacy Impact Assessment

### 1. Introduction

Congress has directed the Executive Branch to establish an integrated entry and exit data system to accomplish the following goals<sup>1</sup>:

1. Record the entry into and exit out of the United States of covered individuals;
2. Verify the identity of covered individuals; and
3. Confirm compliance by visitors with the terms of their admission into the United States.

The Department of Homeland Security (DHS) proposes to comply with this congressional mandate by establishing the United States Visitor and Immigration Status Indicator Technology (US-VISIT) program. The first phase of US-VISIT, referred to as Increment 1, will capture entry and exit information about non-immigrant visitors whose records are not subject to the Privacy Act. Rather than establishing a new information system, DHS will integrate and enhance the capabilities of existing systems to capture this data. In an effort to make the program transparent, as well as to address any privacy concerns that may arise as a result of the program, DHS's Chief Privacy Officer has directed that this PIA be performed in accordance with the guidance issued by OMB on September 26, 2003. As US-VISIT is further developed and deployed, this PIA will be updated to reflect future increments.

### 2. System Overview

#### • What information is to be collected

Individuals subject to the data collection requirements and processes of Increment 1 of the US-VISIT program ("covered individuals") are nonimmigrant visa holders traveling through air and sea ports. The DHS regulations and related Federal Register notice for US-VISIT Increment 1 will fully detail coverage of the program.

The information to be collected from these individuals includes complete name, date of birth, gender, country of citizenship, passport number and country of issuance, country of residence, travel document type (e.g., visa), number, date and country of issuance, complete U.S. address, arrival and departure information, and for the first time, a photograph, and fingerprints. US-VISIT will capture and store this information from existing systems that already record it or are being modified to allow for its collection.

---

<sup>1</sup> Congress enacted several statutory provisions concerning an entry exit program, including provisions in: The Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA) Public Law 106-215; The Visa Waiver Permanent Program Act of 2000 (VWPPA); Public Law 106-396; The U.S.A. PATRIOT Act, Public Law 107-56; and The Enhanced Border Security and Visa Entry Reform Act ("Border Security Act"), Public Law 107-173.

- **Why the information is being collected**

In numerous statutes, Congress has indicated that an entry exit program must be put in place to verify the identity of covered individuals who enter or leave the United States. In keeping with this expression of congressional intent and in furtherance of the mission of the Department of Homeland Security, the purposes of US-VISIT are to identify individuals who may pose a threat to the security of the United States, who may have violated the terms of their admission to the United States, or who may be wanted for the commission of a crime in the U.S. or elsewhere, while at the same time facilitating legitimate travel.

- **What opportunities individuals will have to decline to provide information or to consent to particular uses of the information and how individuals grant consent**

The admission into the United States of an individual subject to US-VISIT requirements will be contingent upon submission of the information required by US-VISIT, including biometric identifiers. A covered individual who declines to provide biometrics is inadmissible to the United States, unless a discretionary waiver is granted under section 212(d)(3) of the Immigration and Nationality Act. Such an individual may withdraw his or her application for admission, or be subject to removal proceedings. US-VISIT has its own privacy officer, however, to ensure that the privacy of all visitors is respected and to respond to individual concerns which may be raised about the collection of the required information. Further, the DHS Chief Privacy Officer will exercise comprehensive oversight of all phases of the program to ensure that privacy concerns are respected throughout implementation. The DHS Chief Privacy Officer will also serve as the review authority for all individual complaints and concerns about the program.

### **3. Increment 1 System Architecture**

US-VISIT Increment 1 will accomplish its goals primarily through the integration and modification of the capabilities of three existing systems:

1. The Arrival and Departure Information System (ADIS)
2. The Passenger Processing Component of the Treasury Enforcement Communications System (TECS)<sup>2</sup>
3. Automated Biometric Identification System (IDENT)

US-VISIT Increment 1 will also involve modification and extension of client software on Port of Entry (POE) workstations and the development of departure kiosks.

The changes to these systems include:

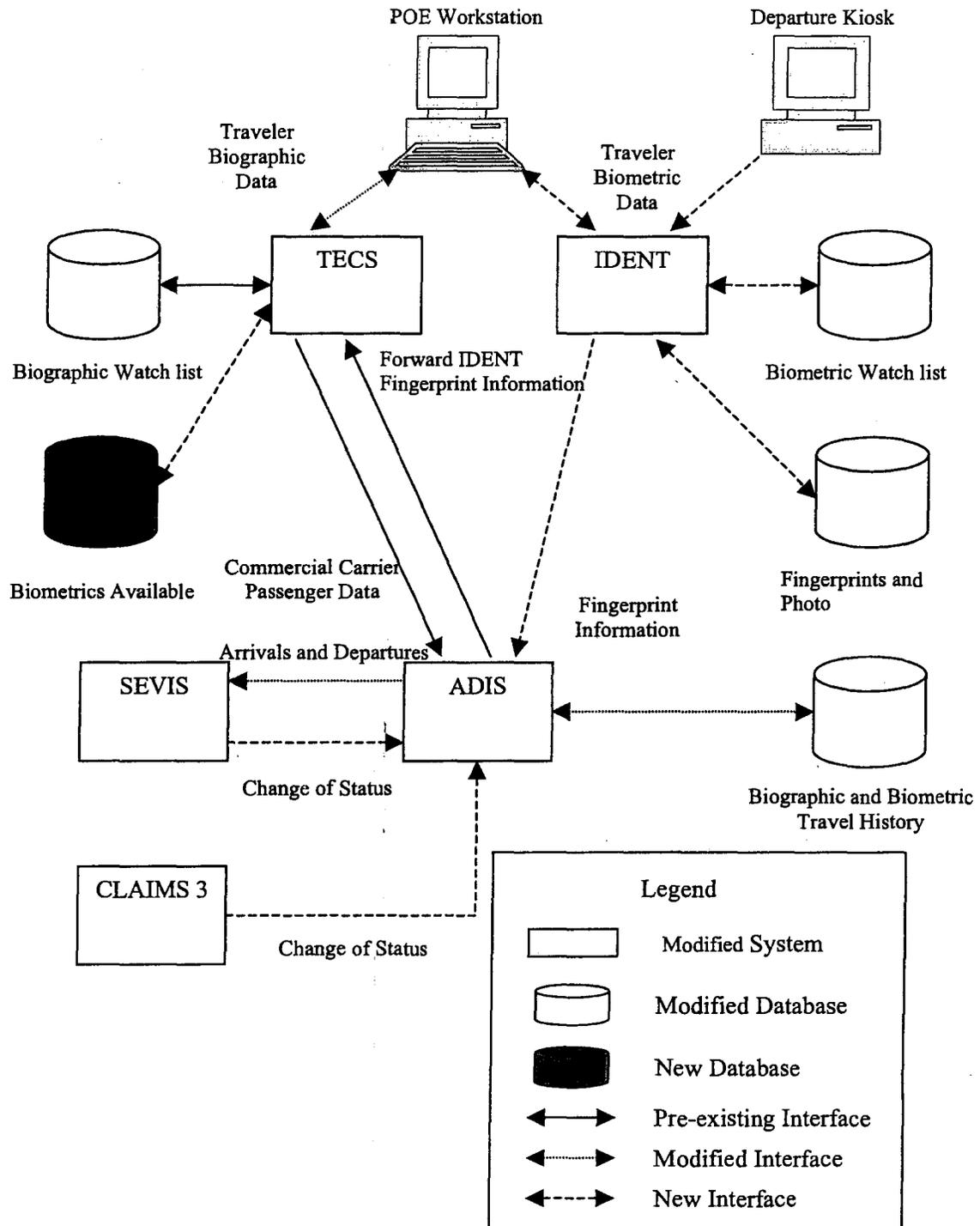
---

<sup>2</sup> As indicated in the US-VISIT Increment 1 Functional Requirements Document (FRD), the Passenger Processing Component of TECS consists of two systems, where "system" is used in the sense of the E-Government Act, title 44, Chapter 35, section 3502 of US Code; i.e., "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." The two systems, and the process relevant to US-VISIT Increment 1 that they support, are (1) Interagency Border Inspection System (IBIS), supporting the lookout process and providing interfaces with the Interpol and National Crime Information Center (NCIC) databases; and (2) Advance Passenger Information System (APIS), supporting the entry process by receiving airline passenger manifest information.

1. Modifications of TECS to give immigration inspectors the ability to display non-immigrant-visa (NIV) data.
2. Modifications to the ADIS database to accommodate additional data fields, to interface with other systems, and to generate various types of reports based on the stored data.
3. Modifications to the IDENT database to capture biometrics at the primary port of entry (POE) and to facilitate identity verification.
4. Establishment of interfaces to facilitate the transfer of biometric information from IDENT to ADIS and from ADIS to TECS.
5. Establishment of other interfaces to facilitate transfer of changes in the status of individuals from two other data bases—the Student and Exchange Visitor Information System (SEVIS) and the Computer Linked Application Information Management System (CLAIMS 3) to ADIS.

Figure 1 presents data flows in the context of the high-level system architecture.

Source: US-VISIT Increment 1 Functional Requirements Document



- **Intended use of the information**

DHS intends to use the information collected and maintained by US-VISIT Increment 1 to carry out its national security, law enforcement, immigration control, and other functions. Through the enhancement and integration of existing database systems, DHS will be able to ensure the entry of legitimate visitors, identify, investigate, apprehend and/or remove aliens unlawfully entering or present in the United States beyond the lawful limitations of their visit, and prevent the entry of inadmissible aliens. US-VISIT thus will enable DHS to protect U.S. borders and national security by maintaining improved immigration control. US-VISIT will also help prevent aliens from obtaining benefits to which they are not entitled.

#### **4. Maintenance and Administrative Controls on Access to the Data**

- **With whom the information will be shared**

The personal information collected and maintained by US-VISIT Increment 1 will be accessed principally by employees of DHS components—Customs and Border Protection, Immigration and Customs Enforcement, Citizenship and Immigration Services, and the Transportation Security Administration—and by consular officers of the Department of State. Additionally, the information may be shared with other law enforcement agencies at the federal, state, local, foreign, or tribal level, who, in accordance with their responsibilities, are lawfully engaged in collecting law enforcement intelligence information (whether civil or criminal) and/or investigating, prosecuting, enforcing, or implementing civil and/or criminal laws, related rules, regulations, or orders. The system of records notices for the existing systems on which US-VISIT draws provide notice as to the conditions of disclosure and routine uses for the information collected by US-VISIT, provided that any disclosure is compatible with the purpose for which the information was collected.

US-VISIT transactions will have a unique identifier to differentiate them from other IDENT transactions. This will allow for improved oversight and audit capabilities to ensure that the data are being handled consistent with all applicable federal laws and regulations regarding privacy and data integrity.

- **How the information will be secured**

The US-VISIT program will secure information and the systems on which that information resides, by complying with the requirements of the DHS IT Security Program Handbook. This handbook establishes a comprehensive program, consistent with federal law and policy, to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, and application rules, which will be applied to component systems, communications between component systems, and at interfaces between component systems and external systems.

One aspect of the DHS comprehensive program to provide information security involves the establishment of rules of behavior for each major application, including US-VISIT. These rules of behavior require users to be adequately trained regarding the security of their systems. These rules also require a periodic assessment of technical, administrative and managerial controls to enhance data integrity and accountability. System users must sign statements acknowledging that they have been trained and understand the security aspects of their systems. In addition, the

rules of behavior already in effect for each of the component systems on which US-VISIT draws will be applied to the program, adding an additional layer of security protection.

The table below provides detail on the various measures employed to address potential security threats to US-VISIT Increment 1.

### Security Threats and Mitigation Methods Detailed

Nature of Threat	Architectural Placement	Safeguard	Mechanism
Intentional physical threats from unauthorized external entities	ADIS	Physical protection	The ADIS database and application is maintained at a Department of Justice Data Center. Physical controls of that facility (e.g., guards, locks) apply and prevent entrée by unauthorized entities.
Intentional physical threats from unauthorized external entities	Passenger Processing Component of TECS	Physical protection	The Passenger Processing Component of TECS is maintained on a mainframe by CBP. Physical controls of the TECS facility (e.g., guards, locks) apply and prevent entrée by unauthorized entities.
Intentional physical threats from external entities	IDENT	Physical protection	IDENT is maintained on an IBM cluster. Physical controls of the facility (e.g., guards, locks) apply and prevent entrée by unauthorized entities.
Intentional physical threats from external entities	POE Workstation	Physical protection	Physical controls will be specific to each POE.
Intentional and unintentional electronic threats from authorized (internal and external) entities	System-wide	Technical protection: Identification and authentication (I&A)	User identifier and password, managed by the Password Issuance Control System (PICS).

## 5. Information Life Cycle and Privacy Impacts

The following analysis is structured according to the information life cycle. For each life-cycle stage—collection, use and disclosure, processing, and retention and destruction—key issues are assessed, privacy risks identified, and mitigation measures discussed. Risks are related to fair information principles—notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress—that form the basis of many statutes and codes.

### • Collection

US-VISIT Increment 1 collects only the personal information necessary for its purposes. While Increment 1 does not constitute a new system of records, it does expand the types of data held in its component systems to include biometric identifiers. By definition this creates a general privacy risk. This risk is mitigated, however, by establishment of a privacy policy supported and enforced by a comprehensive privacy program. This program includes a separate Privacy Officer for US-VISIT, mandatory privacy training for system operators, and appropriate safeguards for data handling.

- **Use and Disclosure**

The IDENT and TECS systems collect data that are used for purposes other than US-VISIT. As a result, data collected for US-VISIT through these systems may become available for another functionality embodied in these component systems. This presents a potential notice risk: will the data be used for a purpose consistent with US-VISIT? This risk is mitigated in several ways. First, US-VISIT isolates US-VISIT data from non US-VISIT data on component systems, and users will be subject to specific privacy and security training for this data. Second, the IDENT and TECS systems already have their own published SORNS, which explain the uses to which the data they collect will be put, for US-VISIT as well as non-US-VISIT purposes. This, too, mitigates the notice risk. Third, Memoranda of Understanding and of Agreement are being negotiated with third parties (including other agencies) that will address protection and use of US-VISIT data, again to mitigate this notice risk.

- **Processing**

Data exchange, which will take place over an encrypted network between US-VISIT Increment 1 component systems and/or applications is limited, and confined only to those that are functionally necessary. Although much of the personal information going into ADIS from SEVIS and CLAIMS 3 is duplicative of data entering ADIS from TECS, this duplication is to ensure that changes in status received from SEVIS or CLAIMS 3 are associated with the correct individual, even in cases of data element mismatches (i.e., differing values for the same data element received from different sources). This mitigates the data integrity risk. A failure to match generates an exception report that prompts action to resolve the issue. This also mitigates integrity risk by guarding against incorrect enforcement actions resulting from lost immigration status changes. (The data flows from SEVIS and CLAIMS 3 principally support changes in status.)

On the other hand, if a match is made, but there are some data element mismatches, no report is generated identifying the relevant records and data elements (one or more of which must have inaccurate or improper values) and no corrective action is taken. This is due to the resources that would be required to investigate all such events. This integrity risk again creates a possibility of incorrect enforcement actions if the match was made in error as a result of the data element mismatches. However, this aspect of the integrity risk is mitigated by subjecting all status changes that would result in enforcement actions to manual analysis and verification. A quality assurance process will also be used to identify any problem trends in the matching process.

- **Retention and Destruction**

The policies of individual component systems, as stated in their SORNS, govern the retention of personal information collected by US-VISIT. Because the component systems were created at different times for different purposes, there are inconsistencies across the SORNS with respect to data retention policies. There is also some duplication in the types of data collected by each system. These inconsistencies and duplication result in some heightened degree of risk with respect to integrity/security of the data, and to access and redress principles, because personal information could persist on one or more component systems beyond its period of use or disappear from one or more component systems while still in use. These risks are mitigated, however, by having a Privacy Officer for US-VISIT to handle specific issues that

may arise, by providing review of the Privacy Officer's decision by the DHS Chief Privacy Officer, and, to the extent permitted by existing law, regulations, and policy, by allowing covered individuals access to their information and permitting them to challenge its completeness. Additionally, as an overarching mechanism to ensure appropriate privacy protections, US-VISIT operators will conduct periodic strategic reviews of the data to ensure that what is collected is limited to that which is necessary for US-VISIT purposes,

US-VISIT Increment 1 will store fingerprint images, both in the IDENT database and transiently on the some POE workstations and departure kiosks. These images are, of course, sensitive, and their storage could present a security as well as a privacy risk. Because retention of fingerprint images is functionally necessary so that manual comparison of fingerprints can be performed to verify biometric watch list matches, appropriate mitigation strategies will be utilized, including encryption on the departure kiosks and physical and logical access controls on the POE workstations and on the IDENT system.

The chart below shows, in tabular form, the privacy risks associated with US-VISIT, Increment One, and the mitigation efforts that will address these risks.

**Privacy Threats and Mitigation Methods Detailed**

Type of Threat	Description of Threat	Type of Measures to Counter/Mitigate Threat
Unintentional threats from insiders <sup>3</sup>	Unintentional threats include flaws in privacy policy definition; mistakes in information system design, development, integration, configuration, and operation; and errors made by custodians (i.e., personnel of organizations with custody of the information). These threats can be physical (e.g., leaving documents in plain view) or electronic in nature. These threats can result in insiders being granted access to information for which they are not authorized or not consistent with their responsibilities.	These threats are addressed by (a) developing a privacy policy consistent with Fair Information Practices, laws, regulations, and OMB guidance; (b) defining appropriate functional and interface requirements; developing, integrating, and configuring the system in accordance with those requirements and best security practices; and testing and validating the system against those requirements; and (c) providing clear operating instructions and training to users and system administrators.
Intentional threat from insiders	Threat actions can be characterized as improper use of authorized capabilities (e.g., browsing, removing information from trash) and circumvention of controls to take unauthorized actions (e.g., removing data from a workstation that has been not been shut off).	These threats are addressed by a combination of technical safeguards (e.g., access control, auditing, and anomaly detection) and administrative safeguards (e.g., procedures, training).

<sup>3</sup> Here, the term "insider" is intended to include individuals acting under the authority of the system owner or program manager. These include users, system administrators, maintenance personnel, and others authorized for physical access to system components.

Intentional and unintentional threats from authorized external entities <sup>4</sup>	<p><b>Intentional:</b> Threat actions can be characterized as improper use of authorized capabilities (e.g., misuse of information provided by US-VISIT) and circumvention of controls to take unauthorized actions (e.g., unauthorized access to systems).</p> <p><b>Unintentional:</b> Flaws in privacy policy definition; mistakes in information system design, development, integration, configuration, and operation; and errors made by custodians</p>	These threats are addressed by technical safeguards (in particular, boundary controls such as firewalls) and administrative safeguards in the form of routine use agreements which require external entities (a) to conform with the rules of behavior and (b) to provide safeguards consistent with, or more stringent than, those of the system or program.
Intentional threats from external unauthorized entities	Threat actions can be characterized by mechanism: physical attack (e.g., theft of equipment), electronic attack (e.g., hacking, interception of communications), and personnel attack (e.g., social engineering).	These threats are addressed by physical safeguards, boundary controls at external interfaces, technical safeguards (e.g., identification and authentication, encrypted communications), and clear operating instructions and training for users and system administrators.

## 6. Summary and Conclusions

Legislation both before and after the events of September 11, 2001 led to the development of the US-VISIT Program. The program is based on Congressional concerns with visa overstays, the number of illegal foreign nationals in the country, and overall border security issues. Requirements for the program, including the implementation of an integrated and interoperable border and immigration management system, are embedded in various provisions of The Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA) Public Law 106-215; The Visa Waiver Permanent Program Act of 2000 (VWPPA); Public Law 106-396; The U.S.A. PATRIOT Act, Public Law 107-56; and The Enhanced Border Security and Visa Entry Reform Act ("Border Security Act"), Public Law 107-173. As a result, many of the characteristics of US-VISIT were pre-determined. These characteristics include:

- Use of a National Institute of Standards and Technology (NIST) biometric standard for identifying foreign nationals;
- Use of biometric identifiers in travel and entry documents issued to foreign nationals, including the ability to read such documents at U.S. ports of entry;
- Integration of arrival/departure data on foreign nationals, including commercial carrier passenger manifests; and
- Integration with other law enforcement and security systems.

<sup>4</sup> These include individuals and systems which are not under the authority of the system owner or program manager, but are authorized to receive information from, provide information to, or interface electronically with the system.

These and other requirements substantially constrained the high-level design choices available to the US-VISIT Program. A major choice for the program concerned whether to develop an entirely or largely new system or to build upon existing systems. Given the legislatively imposed deadline of December 31, 2003 for establishing an initial operating capability, along with the various integration requirements, the program opted to leverage existing systems—IDENT, ADIS, and the Passenger Processing Component of TECS.

As a result of this choice for Increment 1, DHS has determined that a new information system would not be created. Nevertheless, in order to effectively and accurately assess the privacy risks of US-VISIT, and because the program represents a new business process, this Privacy Impact Assessment was performed. In the process of conducting this PIA, DHS identified the need to (1) update the SORNs of the ADIS and IDENT systems to accurately reflect US-VISIT requirements and usage, which has been accomplished, and (2) examine the privacy and security aspects of the existing SORNs and implement any additional necessary strategies to ensure the privacy and security of US-VISIT data.

Based on this analysis, it can be concluded that

- Most of the high-level design choices for US-VISIT Increment 1 were statutorily pre-determined;
- US-VISIT Increment 1 creates a pool of individuals whose personal information is at risk; but
- US-VISIT Increment 1 mitigates specific privacy risks; and
- US-VISIT, through its own Privacy Officer and in collaboration with the DHS Chief Privacy Officer, will continue to track, assess, and address privacy issues throughout the life of the US-VISIT program and update this PIA to reflect additional increments of the program.

### Contact Point and Reviewing Official

Contact Point: Steve Yonkers  
US-VISIT Privacy Officer

(b)(2), (b)(6)

Reviewing Official: Nuala O'Connor Kelly  
Chief Privacy Officer, DHS

(b)(2), (b)(6)

### Comments

We welcome your comments on this privacy impact assessment. Please write to: Privacy Office, Attn.: US-VISIT PIA, U.S. Department Of Homeland Security, Washington, DC 20528, or email [privacy@dhs.gov](mailto:privacy@dhs.gov). Please include US-VISIT PIA in the subject line of the email.

# Appendix

## US-VISIT Program

### Privacy Policy

#### What is the purpose of the US-VISIT program?

The United States Visitor Immigrant Status Indicator Technology (US-VISIT) is a United States Department of Homeland Security (DHS) program that enhances the country's entry and exit system. It enables the United States to record the entry into and exit out of the United States of foreign nationals requiring a visa to travel to the U.S., creates a secure travel record, and confirms their compliance with the terms of their admission.

The US-VISIT program's goals are to:

- a. Enhance the security of American citizens, permanent residents, and visitors
- b. Facilitate legitimate travel and trade
- c. Ensure the integrity of the immigration system
- d. Safeguard the personal privacy of visitors

The US-VISIT initiative involves collecting biographic and travel information and biometric identifiers (fingerprints and a digital photograph) from covered individuals to assist border officers in making admissibility decisions. The identity of covered individuals will be verified upon their arrival and departure.

#### Who is affected by the program?

Individuals subject to the requirements and processes of the US-VISIT program ("covered individuals") are those who are not U.S. citizens at the time of entry or exit or are U.S. citizens who have not identified themselves as such at the time of entry or exit. Non-U.S. citizens who later become U.S. citizens will no longer be covered by US-VISIT, but the information about them collected by US-VISIT while they were non-citizens will be retained, as will information collected about citizens who did not identify themselves as such.

#### What information is collected?

The US-VISIT program collects biographic, travel, travel document, and biometric information (photographs and fingerprints) pertaining to covered individuals. No personally identifiable information is collected other than that which is necessary and relevant for the purposes of the US-VISIT program.

#### How is the information used?

The information that US-VISIT collects is used to verify the identity of covered individuals when entering or leaving the U.S. This enables U.S. authorities to more effectively identify covered individuals that:

- Are known to pose a threat or are suspected of posing a threat to the security of the United States;
- Have violated the terms of their admission to the United States; or
- Are wanted for commission of a criminal act in the United States or elsewhere.

Personal information collected by US-VISIT will be used only for the purposes for which it was collected, unless other uses are specifically authorized or mandated by law.

#### **Who will have access to the information?**

Personal information collected by US-VISIT will be principally accessed by Customs and Border Protection, Immigration and Customs Enforcement, Citizenship and Immigration Services, and Transportation Security Officers of the Department of Homeland Security and Consular Officers of the Department of State. Others to whom this information may be made available include appropriate federal, state, local, or foreign government agencies when needed by these organizations to carry out their law enforcement responsibilities.

#### **How will the information be protected?**

Personal information will be kept secure and confidential and will not be discussed with, nor disclosed to, any person within or outside the US-VISIT program other than as authorized by law and in the performance of official duties. Careful safeguards, including appropriate security controls, will ensure that the data is not used or accessed improperly. In addition, the DHS Chief Privacy Officer will review pertinent aspects of the program to ensure that proper safeguards are in place. Roles and responsibilities of DHS employees, system owners and managers, and third parties who manage or access information in the US-VISIT program include:

##### **1. DHS Employees**

As users of US-VISIT systems and records, DHS employees shall:

- Access records containing personal information only when the information is needed to carry out their official duties.
- Disclose personal information only for legitimate business purposes and in accordance with applicable laws, regulations, and US-VISIT policies and procedures.

##### **2. US-VISIT System Owners/Managers**

System Owners/Managers shall:

- Follow applicable laws, regulations, and US-VISIT program and DHS policies and procedures in the development, implementation, and operation of information systems under their control.
- Conduct a risk assessment to identify privacy risks and determine the appropriate security controls to protect against the risk.
- Ensure that only personal information that is necessary and relevant for legally mandated or authorized purposes is collected.
- Ensure that all business processes that contain personal information have an approved Privacy Impact Assessment. Privacy Impact Assessments will meet appropriate OMB

and DHS guidance and will be updated as the system progresses through its development stages.

- Ensure that all personal information is protected and disposed of in accordance with applicable laws, regulations, and US-VISIT program and DHS policies and procedures.
- Use personal information collected only for the purposes for which it was collected, unless other purposes are explicitly mandated or authorized by law.
- Establish and maintain appropriate administrative, technical, and physical security safeguards to protect personal information.

### **3. Third Parties**

Third parties shall:

- Follow the same privacy protection guidance as DHS employees.

#### **How long is information retained?**

Personal information collected by US-VISIT will be retained and destroyed in accordance with applicable legal and regulatory requirements.

#### **Who to contact for more information about the US-VISIT program**

Individuals whose personal information is collected and used by the US-VISIT program may, to the extent permitted by law, examine their information and request correction of inaccuracies. Individuals who believe US-VISIT holds inaccurate information about them, or who have questions or concerns relating to personal information and US-VISIT, should contact the Privacy Officer, US-VISIT Program, Department of Homeland Security, Washington, DC 20528. Further information on the US-VISIT program is also available at [www.dhs.gov/us-visit](http://www.dhs.gov/us-visit).

**US-VISIT**

Directorate Facilities Points of Contact



Directorate	Directorate Facilities POCs	Phone Number	Office Number
Director's Office	b(6)	b(2), b(6)	
Chief Strategist			
Mission Operations			
Increment Management			
Budget and Finance			
Outreach Management			
Acquisition and Program Management			
Information Technology			
Office of Administration			
Legal and Regulatory Support			

**Attachment 1C**

**DHS US-VISIT Interim Standard Operating Procedures  
for Biometric Enrollment**

TO : Directors, Field Operations  
Director, Preclearance

FROM : Executive Director /s/ Robert Jacksta  
Border Security and Facilitation

SUBJECT: Interim Standard Operating Procedures for United States Visitor and Immigrant Status (US-VISIT) biometric enrollment on January 5, 2004

This memorandum establishes interim Customs and Border Protection (CBP) policy and operating procedures for the US-VISIT biometric enrollment of nonimmigrant arrivals at air and seaports on January 5, 2004. The first phase of US-VISIT, Increment One, requires nonimmigrant visa holders, making an application for admission, to submit biometrics as a condition of entry during the primary inspection process. In addition, Increment One is only applicable at designated air and seaports with primary terminal inspection facilities.

While US-VISIT adds an additional biometric collection requirement to the existing primary inspection process, it does not supersede any operating procedures currently in place.

A. Who is exempt from US-VISIT enrollment?

CBP primary officers will collect fingerprints and photographs from aliens applying for admission with a nonimmigrant visa upon arrival at US-VISIT designated air and seaports. Citizens and Lawful Permanent Residents of the United States are not subject to US-VISIT enrollment requirements and will not be enrolled in US-VISIT.

Applicants for admission that are exempt from documentary requirements pursuant to 8 CFR 212.1 such as citizens of Canada and Bermuda are exempt from US-VISIT enrollment unless applying for admission with a nonimmigrant visa.

Nonimmigrant Mexican visa holders (Border Crossing Cards included) will be enrolled in US-VISIT if entering at designated air and seaports.

Applicants for admission who are citizens from Visa Waiver Program (VWP) participant countries are exempt from US-VISIT enrollment unless applying for admission with a nonimmigrant visa.

Applicants for admission who are in possession of a valid nonimmigrant visa in the A-1, A-2, C-3 (except for attendants, servants or personal employees of accredited officials), G-1, G-2, G-3, G-4, NATO-1, NATO-2, NATO-3, NATO-4, NATO-5 or NATO-6 classifications are exempt from US-VISIT enrollment.

Applicants for admission who are under the age of 14 or over the age of 79 are exempt from US-VISIT enrollment.

Applicants for admission who are subject to the Special Registration Requirements (NSEERS) as specified in 8 C.F.R. 261.1(f)(8) are exempt from US-VISIT enrollment during the primary inspection process. Applicants for admission with an approved waiver for the NSEERS requirement are subject to US-VISIT enrollment.

CBP will make every reasonable effort to accommodate any person with disabilities. Applicant requests for special accommodations to complete primary processing should be referred to secondary. The biometric requirement may be waived at the discretion of the CBP primary officer for applicants with physical limitations, which prevent the collection of the biometrics. If an index fingerprint is amputated, unreadable or injured, then the thumb of the same hand will be utilized. If both are amputated, unreadable or injured then the middle finger is utilized. The ring and little finger are next in sequence if the middle finger is also missing. Applicants for admission expressing privacy concerns are to be referred to secondary for processing.

Applicants who are enrolled and utilize INSPASS will be exempt from US-VISIT enrollment as a biometric is collected.

**B. What happens if an alien refuses to provide the required biometrics?**

A nonimmigrant alien who refuses to provide biometric identifiers when seeking admission to the United States may be deemed inadmissible under the Immigration and Nationality Act (INA), section 212(a) (7) (failure to provide appropriate documents). The nonimmigrant alien's admission is conditioned on compliance with requirement to provide biometric identifiers. A nonimmigrant alien who refuses to provide biometrics at primary or does not understand the process should be sent to secondary for further questioning and any additional processing.

**C. What are the new CBP primary procedures?**

Nonimmigrant aliens subject to US-VISIT enrollment must still undergo a full primary inspection, including all record checks. The CBP primary officer determines identity, examines travel documents, interviews the applicant and completes the primary inspection of various categories of aliens and citizens, including the execution of various forms. This policy does not alter existing guidance on Interagency Border Inspection System/Advance Passenger Information System (IBIS/APIS) or other database queries.

The CBP primary officer is required to scan the entry documents to query against IBIS/APIS. The US-VISIT enrollment process requires the CBP primary officer to capture the biometrics, fingerprints and photograph, of the applicant for admission.

The CBP primary officer is required to scan documents, key information for non-machine-readable documents and correct manifest data if required. IBIS/APIS will return the

results of the biographic query to the primary officer. Each officer will review the query response and respond accordingly. IBIS/APIS will also identify whether a biometric (FIN – Fingerprint Identification Number) has been recorded for the applicant for admission. A new feature of the CBP primary screen will include a nonimmigrant visa image (DataShare), which will be reviewed and compared against all documents provided by the applicant. At this time, the applicant is to be enrolled in US-VISIT. The officer is to toggle to the US-VISIT/IDENT system. The primary officer is required to provide clear professional instructions to the applicant in order to obtain biometric identifiers for comparison. The officer will take two fingerprints, a digital photograph and submit the query to IDENT. The US-VISIT system defaults to collect the left fingerprint first. Each individual officer is responsible for ensuring the correct finger is placed on the scanner. After the officer submits the transmission query to IDENT, the officer will toggle back to IBIS, conduct the interview, await the IDENT query results and respond accordingly. Another new feature of the CBP primary screen include biometric transmission displays of green and red identifiers to assist the officer. The color green indicates no hit found and the color red indicates a referral to secondary is required.

To prevent IDENT biometric data capture errors while performing primary, officers are to ensure that each applicant for admission is processed individually and that each inspection is completed before processing another applicant. This is especially imperative in relation to the inspection of family groups. If an error in biometric data captured is identified, the officer must locate the Form I-94 for the applicant whose biographic information was displayed on the IBIS screen when the incorrect biometric was collected. At this time, biometric error corrections can only occur at the national level. Copies of the Form I-94 are to be faxed to the US-VISIT Technical Team, ATTN: Eve Hermes at primary fax number 202-298-5235 or fax number 202-298-5208. If the Form I-94 is not available, the information required for corrective actions includes: date, location, name, flight number and date of birth.

If an applicant is admitted, the officer will complete IBIS/APIS confirmation, class of admission screen and the corresponding period of the admission. At this time, all applicants for admission at primary even if referred to secondary will be enrolled in US-VISIT. If the applicant is referred to secondary the COA screen will not be completed. Current US-VISIT backend technical procedures will ensure the necessary interfaces to distinguish admitted and refused entries.

The primary officer must identify applicants who may not be admissible or whose inspection will require additional time. The primary officer must communicate with the secondary officer via IBIS, all known information including the basis of the referral.

D. What are the new CBP secondary procedures?

For any applicant referred to secondary due to a US-VISIT IDENT hit, the US-VISIT IDENT Secondary Inspections Tool (SIT) web page ([HTTPS://Apps.ICE.DHS.Gov/VISIT](https://Apps.ICE.DHS.Gov/VISIT)) must be checked to verify the results of any mismatch or watch list biometric hits. This tool will show if the hit has been cleared or verified as a hit. If verified as a hit, it will provide a link to show the watch list or mismatch information. Established IDENT

standard operating procedures state that an expert fingerprint examiner at the Western Identification Network Automated Fingerprint Identification System or Biometric Support Center will complete confirmation on the identity of the primary match and this confirmation will show up in the SIT within ten minutes of the hit on primary.

If the applicant is admitted to the United States, the secondary officer will closeout the primary referral. Secondary officers will include in the comment section of the closeout record the transaction number obtained from the US-VISIT IDENT web page.

If the applicant is determined to be inadmissible to enter the United States, the secondary officer will process the applicant for an adverse action according to established procedures.

E. What is the procedure to report equipment malfunctions or outages?

At this time, system outages, equipment malfunctions or significant US-VISIT response slowdowns will be immediately reported to both the Newington Help Desk at (703) 921-6000 and the CBP US-VISIT Operations Response Desk at (202) 927-1391. Officers are encouraged to consult with the on-site tiger teams who will provide technical and training support during the initial phase of US-VISIT.

F. Summary

CBP primary officers will collect fingerprints and photographs from aliens applying for admission with a nonimmigrant visa upon arrival at US-VISIT designated air and seaports.

Directors and Port Directors are to ensure that CBP officers performing primary inspections are aware of this memorandum. Supervisory and/or management officials will ensure that officers are familiar with and comply with, the contents of this memorandum.

If you have any further questions regarding the procedures outlined in this memorandum please contact (b)(6) Border Security and Facilitation, at (b)(2), (b)(6)

**Attachment 2**  
**DHS Biometrics Survey: SENTRI Pedestrian Test**

**Please identify the program/initiative and the purpose for using biometrics.**

SENTRI pedestrian test.

**What is the type of biometrics technology used?**

Border Security and Facilitation will plan to test a new concept where facial and fingerprint recognition will be tested in the primary inspection process at the San Ysidro Port of Entry in early fall 2004.

**How much did it cost your agency to implement the use of biometrics for the program/initiative and what is the FY04 projected cost for using the technology?**

This is only a test and there are no funds appropriated.

**Is the use of biometrics for this program or initiative mandated by statute or rule?**

No.

**How is the biometrics information gathered collected, and stored?**

The information and biometrics will be gathered and stored in the same manner as the current SENTRI enrollment process used for facilitating entry to vehicle occupants.

**Is the information accessible by other agencies or other entities (including contractors, vendors, and state and local governments)?**

No, the information will be safeguarded in the same manner as the current SENTRI program as described above. The information will be made accessible only to those who are representatives of the contractor installing the application.

**Please describe the security measures used to protect the biometric information that is gathered, including any limitations on accessing the information.**

The information will be compliant to security measures as outlined by current OIT policy as is to the existing SENTRI vehicle program.

**Did your agency conduct any privacy assessments for this use of biometrics?**

No.

**At what rate have false-positives been returned during the use of biometrics in this program?**

None.

**What is the process in place to ensure that there is not repeated false-positives in the system?**

None.

**Attachment 3  
DHS Biometrics Survey: TSA TWIC**

***Note: TWIC will commence Prototype Phase in May 04; therefore, information provided herein represents the systems current conceptual capability only.***

**Please identify the program/initiative and the purpose for using biometrics**

The Transportation Security Administration (TSA) is developing the Transportation Worker Identification Credential (TWIC) System to improve security by developing an integrated credential-based identity management system. The target audience includes transportation workers requiring unescorted physical access to secure areas of the nation's transportation system, as well as logical (cyber) access to networks and systems. As envisioned, the requirements for this credential will include: verification of each TWIC holder's identity, completion of a successful background check, and linking each credential to its rightful holder through the use of biometric technology. The purpose of collection is for identity verification (1:1) and to prevent alias enrollments (1:N). Fingerprint scans and facial image capture will be used.

**What is the type of biometrics technology used?**

For Prototype Phase, the primary device will collect 8 finger images for 1:N search. The state of Florida will continue to collect 10-prints with existing CrossMatch livescan devices to satisfy statutory requirements. TWIC Prototype Phase will evaluate biometric readers for access control in and around transportation facilities, and for 1:1 identity verification. TWIC will consist of a smartcard with embedded Integrated Circuit Chip or ICC. Additionally, the Prototype Phase includes use and evaluation of iris as a reference biometric.

**How much did it cost your agency to implement the use of biometrics for the program/initiative and what is the FY04 projected cost for using the technology?**

No expenditure to date. Projected costs will be available at conclusion of Prototype Phase.

**Is the use of biometrics for this program or initiative mandated by statute or rule? If YES, reference the statutory or regulatory citation.**

Yes, the Maritime Transportation Security Act (MTSA), 2002 (PL 107-295), § 101 and 70105, and the Aviation and Transportation Security Act (PL 107-71—NOV. 19, 2001) § 106 and 109.

**How is the biometrics information gathered, collected, and stored?**

Fingerprint biometrics information is collected during enrollment process. The fingerprint images are securely stored in a segmented database that prevents the association of an

image with demographic/biographic information. Additionally, templates are stored on the ICC of the TWIC for identity verification via 1:1 match and protected using public key cryptography.

**Is the information accessible by other agencies or other entities (including contractors, vendors, and state and local governments)?**

Not "accessible" but eventually background checks will require biometrics to be submitted to appropriate agencies to conduct a background investigation.

**Please describe the security measures used to protect the biometric information that is gathered, including any limitations on accessing the information.**

All processes and transactions are recorded to ensure privacy safeguards were properly employed on all individual enrollments. Auto-delete functions are applied in data flow process to assure appropriate removal of personal data from local workstations. All data is encrypted in transmission, and at rest. Fingerprint images are stored in electronically and physically segmented databases that effectively disassociate fingerprint images from personal demographic/biographic information. On-card reference biometric templates are encrypted. Access privileges are biometrically secured. Only the highest-level authorities will have access to personal data. The following standards will be followed:

- National Institute of Science and Technology (NIST)
- American National Standards Institute (ANSI)
- Federal Information Processing Standards 140, as applicable
- Government Smart Card Interoperability Specification (GSC-IS)
- International Organization for Standardization (e.g. ISO 7810, 7816, 14443, 15693)
- Security Equipment Integration Working Group (SEIWG 012)
- INCITS 383 Biometric Profile - Interoperability and Data Interchange-Biometrics-Based Verification and Identification of Transportation Workers

It is the intention of the TWIC Program to follow the guidance of relevant government standards bodies related to protecting privacy, including the Government Smart Card – Interagency Advisory Board (GSC-IAB) and the Physical Access Interagency Interoperability Working Group (PAIIWG), and make use of all impending standards work that may involve personal data security.

**Did your agency conduct any privacy assessments for this use of biometrics? If so, please attach copies of any relevant assessments.**

A TWIC Privacy Impact Assessment is currently in draft form and will be refined during the course of Prototype, and after system architecture and design is completed.

**At what rate have false-positives been returned during the use of biometrics in this program?**

To be evaluated during Prototype Phase. Anticipate results end of CY04.

**What is the process in place to ensure that there is not repeated false-positives in the system?**

If applicable, processes will be developed based on performance results of Prototype Phase.

**Attachment 4**  
**DHS Biometrics Survey: TSA RT and Armed LEO Pilot**

The Department of Homeland Security will be collecting biometrics from voluntary participants as part of the **Registered Traveler and Armed LEO Pilot Programs**. The Transportation Security Administration (TSA) plans to implement the RT Pilot at a limited number of airports beginning in June 2004. These pilot programs will be coordinated through TSA's Credentialing Program Office (CPO). The following responses pertain to these pilot operations, as currently envisioned.

**Please identify the program/initiative and the purpose for using biometrics.**

The RT and Armed LEO Pilots will use biometrics to enhance the security and efficiency of passenger and LEO screening operations. Biometrics will be used as an identity management tool for identity verification for known travelers enrolled in the pilot program. The biometric samples collected will be run against terrorist watch lists and potentially against criminal databases. In addition, biometrics will be used for identification of federal law enforcement officers participating in the pilot.

**What is the type of biometrics technology used?**

Based upon guidance received from the Transportation Security Lab (TSL), the CPO has selected two biometrics that are potentially capable of meeting the RT / Armed LEO Pilot requirements in the most timely and cost effective manner: **fingerprint and iris recognition**.

The CPO has worked closely with the Transportation Security Lab (TSL) and other industry experts to identify biometric technologies that may meet the unique business, functional, and security requirements of the RT and Armed LEO projects.

**How much did it cost your agency to implement the use of biometrics for the program/initiative and what is the FY04 projected cost for using the technology?**

The FY04 budget supporting the pilot implementation, which includes biometric technology, is approximately \$5M. The requested program budget for FY05 is \$15M. This will be used to implement Registered Traveler program at a national level. The goal after FY05, is to have the RT Program become self-funding through enrollment fees. No funding has been allocated to the Armed LEO Program.

**Is the use of biometrics for this program or initiative mandated by statute or rule? If YES, reference the statutory or regulatory citation.**

The use of biometrics for this program is not mandated by a statute or rule. However, under the Aviation and Transportation Security Act (ATSA) of November 2001, Section 109, TSA has been tasked with the evaluation and, as appropriate, the implementation of a "traveler" system, using available technologies to expedite security screening of passengers who participate, and the subsequent improved allocation of screening

resources to focus on those passengers who should be subject to more extensive screening. TSA believes that the most effective way of achieving that goal is by the use of biometric technology.

**How is the biometrics information gathered, collected, and stored?**

Biometric information will be gathered for all pilot participants during the enrollment process. Enrollment will likely occur at the airport pilot sites. This information will be stored on a secured Smart Card or other credential or token (government or non-government). In addition, TSA will utilize a database to store the master list of pilot participant data. This database is currently being designed, and will include provisions to ensure that the data will be stored in a secured manner.

**Is the information accessible by other agencies or other entities (including contractors, vendors, and state and local governments)?**

Information gathered for the RT and Armed LEO Pilots will be shared with Federal, State and local government agencies to ensure safety and security, assess and distribute intelligence or law enforcement information related to transportation security, assess and respond to threats to transportation.

The information will be accessible to contractors, grantees, experts, consultants, or volunteers when necessary, to perform a function or service related to this system of records for which they have been engaged. Such recipients are required to comply with the Privacy Act, 5 U.S.C. 552a, as amended.

In addition, pilot participant information can be accessed by a Federal, State, local, tribal, territorial, foreign, or international agency, in response to queries regarding persons who may pose a risk to transportation or national security; a risk of air piracy or terrorism or a threat to airline or passenger safety; or a threat to aviation safety, civil aviation, or national security.

Finally, information will be accessible to the General Services Administration and the National Archives and Records Administration in records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

**Please describe the security measures used to protect the biometric information that is gathered, including any limitations on accessing the information.**

Information in this system is safeguarded in accordance with applicable rules and policies, including any applicable TSA and DHS automated systems security and access policies. The computer system from which records could be accessed will be policy and security based, meaning access is limited to those individuals who require it to perform their official duties. Classified information is appropriately stored in a secured facility, secured databases, and containers and in accordance with other applicable requirements, including those pertaining to classified information.

**Did your agency conduct any privacy assessments for this use of biometrics? If so, please attach copies of any relevant assessments.**

At this time, the agency is in the process of conducting a Privacy Impact Assessment for the RT Pilot Program that will be published in the Federal Register. This assessment has not yet been finalized. A CPO privacy representative has been designated to support all credentialing-related programs, including the Registered Traveler Pilot.

**At what rate have false-positives been returned during the use of biometrics in this program?**

This Pilot Program has not been launched; therefore this information is not yet available.

**What is the process in place to ensure that there is not repeated false-positives in the system?**

As mentioned above, this does not yet apply to the RT Pilot Program. We will have an answer to that question as the test program develops.

**Attachment 5**  
**DHS Biometrics Survey: USCIS**

DHS collects biometrics from persons applying to U.S. Citizenship and Immigration Services (USCIS) for benefits. The following responses pertain to this program.

**Please identify the program/initiative and the purpose for using biometrics**

USCIS collects biometrics (10-prints, photo, signature, and single press-print) at Application Support Centers (ASCs) and Service Center scanning stations in connection with a variety of benefit programs, including naturalization, adjustment of status, temporary protected status, permanent resident card ("green card") renewal and replacement, and international adoption.

- 10-print civil images are used to conduct criminal background checks with the FBI.
- Photos, signatures and single press-prints are used to produce various documents issued by USCIS, such as Employment Authorization Documents (EADs) and Permanent Resident Cards (PRCs). In addition, when USCIS documents are created, the biometric images used to construct the documents are deposited in the Image Storage and Retrieval System (ISRS) through which visual identity verification is performed on certain applicants.

**What is the type of biometrics technology used?**

USCIS uses the following biometrics technology:

- Fingerprints (10-prints on a Civil FD-258) for criminal history checks.
- ¾ profile color digital photo, signature, and right index press-print for various cards and travel documents.

**How much did it cost your agency to implement the use of biometrics for the program/initiative and what is the FY04 projected cost for using the technology?**

USCIS spent \$120 million to establish the Application Support Center program in FY98. The FY04 budget supporting the capture and use of biometrics is approximately \$90M.

**Is the use of biometrics for this program or initiative mandated by statute or rule? If YES, reference the statutory or regulatory citation.**

The use of biometrics (photographs and fingerprints) is based on multiple statutory and regulatory mandates. These include: Public Law 105-277; Title 8 of the U.S. Code; and 8 CFR 103.2, 264, 245, 245a, 316, etc.

**How is the biometrics information gathered, collected, and stored?**

Biometrics are gathered through two venues as follows:

- (1) Customers applying for certain immigration benefits are scheduled to appear at an Application Support Center where 10-prints, a photograph, signature, and a press-

print are collected. (In some instances customers supply hardcopy photo with their application, which is later converted into electronic format.) The 10-prints are transmitted to the FBI for a criminal history check. The fingerprint images are currently retained on data tapes by USCIS, and the transaction data, the biographic information, and the fingerprint response is stored in a fingerprint tracking system. The fingerprint images are not readily accessible.

(2) The photo, signature, and press-print are used to construct documents, such as EADs, and PRCs, issued by USCIS. The biometrics are retained in the ISRS and are available for view-only purposes.

USCIS is developing a Biometric Storage System (BSS) that will house all biometrics collected by the agency and support reuse of the images. The fingerprint images now being collected will be available in the BSS.

*Note: Not all of the biometrics listed above are captured for all customers. In some instances, only 10-prints or the photo are captured.*

**Is the information accessible by other agencies or other entities (including contractors, vendors, and state and local governments)?**

USCIS makes the following biometric data accessible to other agencies or entities:

- 10-prints to the FBI for criminal background checks on benefit applicants
- Photo, signature and fingerprints to CBP/US-VISIT for identity verification at ports of entry
- Contractors who support the benefits systems

*Note: Application Support Centers are USCIS managed facilities, but staffed by contract personnel.*

**Please describe the security measures used to protect the biometric information that is gathered, including any limitations on accessing the information.**

Access to the ISRS and the fingerprint system is on a password-control basis only. Each transaction is logged and auditable. The systems are in full compliance with legacy INS security standards.

**Did your agency conduct any privacy assessments for this use of biometrics? If so, please attach copies of any relevant assessments.**

USCIS conducted a privacy impact assessment for its citizenship and immigration benefit processing systems. This assessment (attached) addressed the use of biometrics.

**At what rate have false-positives been returned during the use of biometrics in this program?**

No instances of false-positives have been noted.

**What is the process in place to ensure that there is not repeated false-positives in the system?**

N/A – see above

**Please provide a copy of any procedures or policies your agency has in place regarding the use of biometrics. If these procedures or policies are program or initiative specific, please indicate so.**

USCIS has program specific policies and procedures in place on the use of biometrics for adjudicating applications for citizenship and certain immigration benefits. These programs include, but are not limited to: naturalization, adjustment of status, temporary protected status, permanent resident card (“green card”) renewal and replacement, and international adoption. The vast variety of policy and procedural documents that address USCIS use of biometrics for these programs are too voluminous to attach to this survey, but can be located at <http://uscis.gov/graphics/lawsregs/index.htm>.

**Attachment 5A**  
**USCIS Privacy Impact Assessment**  
**(See Document under Separate Cover)**

Department of Homeland Security

United States Citizenship and Immigration Services



Privacy Impact Assessment  
Benefit Processing Systems

January 31, 2004



**TABLE OF CONTENTS**

**TABLE OF CONTENTS** ..... iii

**INTRODUCTION**.....1

    PURPOSE ..... 1

    SCOPE 2

    BACKGROUND.....2

    DOCUMENT ORGANIZATION .....2

    DOCUMENT MAINTENANCE .....3

**SYSTEM PRIVACY REQUIREMENTS AND RELATED DOCUMENTS**.....4

    FEDERAL REQUIREMENTS AND GUIDANCE .....4

    DHS REQUIREMENTS AND GUIDANCE .....4

    USCIS SECURITY-RELATED DOCUMENTS .....5

**PIA METHODOLOGY**.....6

    ROLES AND RESPONSIBILITIES .....6

    IDENTIFYING PERSONAL INFORMATION .....7

    PIA QUESTIONNAIRE .....8

    PIA OBSERVATIONS AND RECOMMENDATIONS .....9

    PIA CONCLUSIONS .....9

**SYSTEM IDENTIFICATION**.....10

    SYSTEM OVERVIEW .....10

    GENERAL DESCRIPTION AND PURPOSE .....10

    MAJOR SYSTEM COMPONENTS AND INTERCONNECTIONS .....12

    INFORMATION SHARING .....12

    INFORMATION SENSITIVITY .....12

**OBSERVATIONS AND RECOMMENDATIONS** .....14

    SYSTEM CHARACTERIZATION .....14

    INFORMATION SHARING PRACTICES .....14

    WEB SITE HOST .....15

    ADMINISTRATIVE CONTROLS .....15

    TECHNICAL CONTROLS .....16

    PHYSICAL CONTROLS.....16

**CONCLUSION** .....17

**APPENDIX A - ACRONYMS** .....18

**APPENDIX B - DEFINITIONS** .....21

**APPENDIX C - REFERENCES**.....23

**APPENDIX D – PIA QUESTIONNAIRE – CLAIMS 3** .....24

**APPENDIX D – PIA QUESTIONNAIRE – CLAIMS 4** .....42

**APPENDIX D – PIA QUESTIONNAIRE -- RNACS**.....60

**APPENDIX D – PIA QUESTIONNAIRE -- RAPS** .....78

**APPENDIX D – PIA QUESTIONNAIRE – MFAS**.....60

**APPENDIX E – INFORMATION SHARING DATA ELEMENTS .....114**  
**APPENDIX F – USER ROLES .....117**

## **EXECUTIVE SUMMARY**

This document constitutes the PIA Report for USCIS for the Computer Linked Automated Information Management System (CLAIMS 3 and CLAIMS 4), the Refugees, Asylum, and Parole System (RAPS), the Reengineered Naturalization Casework System (RNACS), and the Marriage Fraud Amendment Act System (MFAS) and addresses privacy issues, as required by the Federal Government, DHS, and USCIS. These five systems are being addressed in one PIA because together they make up the current case processing system used by USCIS to process all applications that are processed electronically.

The threshold for conducting a PIA was met by two of the systems. CLAIMS 3 contains PII and will have a major change with the addition of an intranet site for National Benefits Center access. RAPS contains PII and the system will be modified to allow for automating the process of creating notifications to applicants without representing a new collection of information. RAPS will also be updated to share the results of asylum requests, including names, etc, with Canada. The other three systems (CLAIMS 4, RNACS, and MFAS) do not meet the PIA threshold but are included in this PIA because they contain the same type of information, used in the same way as the other two systems.

A total of five specific deficiencies requiring remediation were identified. These include a lack of notification of other resources when PII is changed, a lack of review of PII within the system, the lack of a system security plan for CLAIMS 3, a lack of password controls for all systems except CLAIMS 4, and a lack of incident reporting for RNACS and RAPS.

## INTRODUCTION

The United States Citizenship and Immigration Services (USCIS) is responsible for providing proper protections for the information contained within its information systems, including personally identifiable information (PII). Because the various systems used by USCIS contain PII, USCIS has conducted this Privacy Impact Assessment (PIA) to assess whether the system meets legal privacy requirements. The PIA methodology, the PIA Questionnaire used to implement the methodology, and the assessment results are provided here.

This PIA complies with Federal, Office of Management and Budget (OMB), Department of Homeland Security (DHS), and USCIS requirements. It also serves as an important document supporting USCIS Information Technology Investment Management (ITIM) decision points.

At the time of this PIA, many variables exist that will affect the systems and the privacy requirements they must meet. These variables include:

- The new Benefits Application Processing System being developed by USCIS that will replace the systems included in this PIA.
- Changes in information privacy requirements, particularly with respect to possible new requirements from the Department and the further PIA guidance from OMB.
- Changes resulting from the re-organization of the former Immigration and Naturalization Service (INS), now known as USCIS, into the Department of Homeland Security (DHS).

### Purpose

The PIA process is used to evaluate privacy vulnerabilities and risks, and their implications for information systems. PIAs provide benefits including enhancing policy decision-making and system design, anticipating the public's possible privacy concerns, and generating confidence that privacy objectives are addressed in the development and implementation of single-agency or integrated information systems. The PIA Questionnaire provides a framework by which USCIS can ensure system compliance with all relevant privacy policies, regulations, and guidance, both internal and external to USCIS and DHS.

The PIA process guides system owners and developers in assessing information systems through all phases of the System Development Life Cycle (SDLC). According to OMB, a PIA should be performed before developing or procuring information technology or when initiating a new collection of information in identifiable form for ten or more persons. A PIA should also be conducted or an existing PIA updated at any time the system is significantly modified or the sensitivity of the data contained within the system is changed.

For the PIA, all procedures that address the use, storage, retrievability, accessibility, retention, and disposal of PII are examined. The assessment requires that the system owners and developers answer privacy-related questions regarding the data in the system, access to the data, attributes of the data, characteristics of the system, and maintenance of administrative, technical and physical controls.

## Scope

This document constitutes the PIA Report for USCIS for the Computer Linked Automated Information Management System (CLAIMS 3 and CLAIMS 4), the Refugees, Asylum, and Parole System (RAPS), the Reengineered Naturalization Casework System (RNACS), and the Marriage Fraud Amendment Act System (MFAS) and addresses privacy issues, as required by the Federal Government, DHS, and USCIS. These five systems are being addressed in one PIA because together they make up the current case processing system used by USCIS to process all applications that are processed electronically.

## Background

CLAIMS 3 and CLAIMS 4 are used by USCIS to process benefit applications, RAPS is used to adjudicate asylum applications, RNACS is used to process some naturalization applications, and MFAS is used to adjudicate petitions covered by the Immigrant Marriage Fraud Act (IMFA) of 1986. Currently, USCIS receives between six and nine million applications per year from individuals seeking benefits such as employment authorization, permanent residency in the United States, or United States citizenship.

## Document Organization

This document consists of the following sections and appendices:

- Section 1, Introduction, introduces the document's purpose, scope, and contents, and how the document is to be maintained.
- Section 2, System Privacy Requirements and Related Documents, describes privacy requirements and lists related documents.
- Section 3, PIA Methodology, describes the PIA methodology and the roles and responsibilities of those persons involved in preparing the final PIA, and discusses defining and identifying PII residing on USCIS systems.
- Section 4, System Identification, characterizes the system, including system name, overview, general description and purpose, major components (including hardware and software), system interconnections, information sharing and the sensitivity of information contained in the system.
- Section 5, PIA Results and Recommendations, documents PIA findings according to the seven categories used in the PIA Questionnaire and analyzes the impact of any weaknesses/deficiencies and the privacy issues raised by the review, and discusses recommendations and options available to remove or mitigate identified risks.
- Section 6, Conclusion, discusses conclusions drawn from the PIA results; factors that will affect the system and the PIA in the future, and subsequent PIA report activities.
- Appendix A, Acronyms, lists the acronyms used throughout this document.
- Appendix B, Definitions, provides definitions for terms used throughout this document.
- Appendix C, References, lists the references used throughout this document.

- Appendix D, PIA Questionnaires, consists of questions that attempt to determine what kind of PII is contained within the system, what is done with that information, and how that information is protected.
- Appendix E, Information Sharing Data Elements, lists those types of data elements that may be shared with other resources or entities.
- Appendix F, User Roles, lists the various users who to have access to the systems and their functions with respect to the system.

### **Document Maintenance**

This PIA will be maintained by USCIS. Additionally, the PIA should be updated as new guidelines are made available as the result of new legal requirements such as the E-Government Act of 2002.

## SYSTEM PRIVACY REQUIREMENTS AND RELATED DOCUMENTS

This USCIS PIA complies with the statutory and regulatory requirements currently in place for Federal agencies. Where guidance exists, at the Federal Government level, at the Department level, and from recognized non-government sources, this PIA seeks to follow that guidance. The laws, regulations and guidance documents used to conduct this PIA are listed below. Statutory and regulatory privacy and related security references are also noted in the PIA Questionnaire and cross-referenced in the PIA results.

USCIS recognizes that PIA requirements are likely to change as DHS develops new guidance and OMB releases follow-on privacy and web-privacy-related guidance. By conducting this baseline PIA and establishing a PIA process for future reviews, USCIS has placed itself in the appropriate position to adopt and adapt to new requirements and guidance.

### Federal Requirements and Guidance

The Privacy Act of 1974, along with its accompanying case law, is the foundation statute mandating the protection of the privacy of personal information held by the Federal government. The Privacy Act establishes fair information practices for collecting, maintaining and using personal information by Federal agencies.

Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. 36) requires that a PIA be done for each new information system and for existing systems as major changes are made. Section 208 outlines required PIA content, directs the OMB Director to issue further guidance; and requires the Department's Chief Privacy Officer (CPO) to review and, where possible, make the PIA publicly available. On September 30, 2003, OMB released final guidance providing information to agencies on implementing the privacy provisions of the E-Government Act of 2002 and updating and consolidating existing guidance on agency web site privacy policies. Where indicated, this guidance modifies and replaces OMB guidance found in the following memoranda: OMB M-99-05, OMB M-99-18, and OMB M-00-13.

Other relevant Federal guidance regarding privacy protections for personal information includes:

- OMB Circular A-130, *Management of Federal Information Resources*, February 8, 1996 - provides instructions to Federal agencies for complying with the fair information practices and security requirements for operating automated information systems.
- OMB Circular A-11, *Exhibit 300* – requires that a privacy risk assessment be performed and accompany revised Exhibit 300s for budget requests.
- *Internal Revenue Service Model Information Technology Privacy Impact Assessment*, 1996 – recognized by the Federal Chief Information Officer (CIO) Council as the Government Best Practice for conducting an information system PIA.

### DHS Requirements and Guidance

DHS has recently appointed a Privacy Officer who will seek to balance public safety, public access, and privacy when developing information policies and procedures for DHS components or integrated DHS systems. As privacy guidance is developed and approved by the Department, USCIS will ensure that requirements are properly implemented and enforced.

**USCIS Security-Related Documents**

This PIA is part of a suite of documents developed and maintained for USCIS, which includes:

- CLAIMS 4, Functional Requirements Document, April 1999.
- CLAIMS 4, System Design Document, April 2000.
- CLAIMS 4, Requirements Traceability Matrix, January 2004.
- Refugee, Asylum and Parole System (RAPS) Functional Requirements Document, December 1992
- Computer Linked Application Information Management System 3 – Mainframe (CLAIMS 3 – MF) and Marriage Fraud Assessment System (MFAS), Risk Assessment, November 2003
- Computer Linked Application Information Management System 3 – Mainframe (CLAIMS 3 – MF) and Marriage Fraud Assessment System (MFAS), Sensitive System Security Plan, November 2003

## PIA METHODOLOGY

The PIA methodology includes the following steps:

1. Identify PIA roles and responsibilities.
2. Identify PII handled by the USCIS systems covered by this PIA.
3. Complete the PIA Questionnaire using system documentation and information provided by system developers and administrators in one-on-one and group interviews.
4. Report the PIA results discussing the system attributes, outlining the high-level findings of the PIA Questionnaire, and analyzing the privacy issues raised and options available for mitigating identified risks. The PIA Report is submitted with the completed PIA Questionnaire as an appendix. Both the CIO and the Privacy Officer review the PIA results. Upon completion, the PIA Report is considered Sensitive But Unclassified (SBU) information.
5. Once the PIA Report has been completed, USCIS should revise their information system security Plan of Actions and Milestones (POA&M) to include those mitigating actions identified through the PIA process.
6. USCIS will then perform the mitigation actions in accordance with the POA&M and update the POA&M as necessary.

### Roles and Responsibilities

Every federal employee and contractor who comes into contact with information in identifiable form is responsible for maintaining information privacy.

#### DHS Chief Privacy Officer

Direct the overall implementation of the Privacy Act and privacy policy for the Department. Field questions regarding privacy issues arising from the completion of the PIA and the implications of the management of PII contained in USCIS information systems. Completed PIAs will be provided to the Chief Privacy Officer.

#### Agency Head

Ensure that appropriate privacy safeguards are provided for the information contained within its systems. USCIS is responsible for performing PIAs on its information systems. Once any privacy vulnerabilities or areas of noncompliance have been identified, USCIS must update the system POA&M to incorporate the actions necessary to resolve privacy issues.

Inform and educate all employees and contractors of their responsibility for protecting information in identifiable form; Identify those individuals in the agency (e.g., Privacy Officers, information technology personnel) that have day-to-day responsibility for overseeing implementation of section 208 of the E-Government Act, the Privacy Act, or other privacy laws and policies.

Designate a “*reviewing official*” for each IT system or information

	collection requiring a PIA (the <i>agency CIO</i> or other official designated by the head of the agency), to review the PIA analysis and resulting determinations.
<b>USCIS Office of the Senior IT Officer (OSITO)</b>	Coordinate PIA activities within the USCIS and provide guidance to ensure the methodology is implemented consistently. Review PIA findings and serve on the PIA Review Team. Ensure that all identified privacy vulnerabilities and areas of noncompliance have been documented and resolution tracked through the POA&M process.
<b>USCIS Privacy Officer</b>	Review PIA findings, interpret privacy law and policy, and serve on the PIA Review Team.
<b>USCIS Legal Counsel</b>	Review PIA findings, interpret privacy law and policy, and serve on the PIA Review Team.

### Identifying Personal Information

One goal of federal privacy laws and regulations is ensuring that PII is protected from unauthorized access and disclosure. For purposes of this PIA, PII is defined as any information that can be used to identify a specific individual. These data include, but are not limited to, social security numbers, driver's license numbers, health records, legal records, financial records, and biometric information.

The first step in conducting a PIA is data analysis or determining if PII is handled by a system and if so, what type of information it is. Data analysis first requires mapping pieces of information as they flow through the system, allowing USCIS to understand what types of information are received or collected and from where, in what context that information is used, whether it is personally identifiable and when and to whom it may be disseminated.

After mapping the data flow, data analysis next requires USCIS to determine the attributes, or sensitivity, of the PII handled by the systems to determine the appropriate use and dissemination of that information. The system sensitivity level is 3 for CLAIMS 3, CLAIMS 4, RAPS, RNACS, and MFAS. The DHS has determined that the information accessed by these systems is sensitive but unclassified (SBU). The systems processes SBU information and so are required to have the functionality of controlled access protection (C2) level of trust as defined in Department of Defense (DOD) 5200.28, *DOD Trusted Computer Systems Evaluation Criteria*.

The type of personal information collected, used, and maintained will determine which privacy laws, if any, are invoked and how USCIS will decide how to handle that information. The Privacy Act, for example, is potentially invoked when one or more data elements listed below are contained in a record. If, however, a record contains personal medical information about an individual, the Health Insurance Portability and Accountability Act (HIPAA) may also be applicable.

Data elements may include but are not limited to:

- Name
- Social Security Number (or other identifying number originated by the Government)
- Alien Number (A-Number)
- Date of Birth
- Photographic Identifier (e.g., picture, photo image, X-ray, and video)
- Biometric Identifier (e.g., fingerprint and voiceprint)
- Drivers license number
- Certificates (birth, death, and marriage)
- Mother's Maiden Name
- Postal and Mailing Address
- Phone Numbers
- Education Records
- E-mail Address
- Employment History (e.g., place of employment, salary, and evaluations)
- Medical Records and Notes (e.g., prognosis, prescriptions, treatments related to an individual, and device identifiers)
- Financial Account Numbers (e.g., checking account and personal identification number (PIN))

### PIA Questionnaire

In completing the PIA Questionnaire, USCIS may choose to consult existing system documentation and system developer(s), administrator(s) and users to obtain the most accurate characteristics of the system. Where they exist, past reports regarding the system's security (e.g., certification and accreditation (C&A) reports, Government Information Security Reform Act (GISRA) and Federal Information Systems Management Act (FISMA) reports, and risk assessments) may be helpful in answering some question sets, especially the administrative, technical, and physical controls questions. The system owners will consult such reports as do exist for the system to complete the PIA. The system owners will also consult with the DHS and/or USCIS privacy officer(s) for clarification of Privacy Act-related compliance issues and interpretation of Federal case law related to completion of this PIA.

To ensure the system complies with the appropriate authorities, the PIA Questionnaire first characterizes the systems. The types of information contained on the system are then identified; information-sharing practices are evaluated; and system controls for administrative, technical, and physical safeguards are assessed to ensure the system is adequately protected. Where relevant, any Federal privacy law(s) and/or DHS and USCIS privacy policies driving the business requirement are referenced in that question set.

Additionally, where questions carry consequences for noncompliance, the PIA Questionnaire provides high-level remediation guidance for implementing privacy corrective actions. Where clarification or system details are required, the question box notes the need for more information and asks the PIA user to elaborate in the comments section.

### **PIA Observations and Recommendations**

This step constitutes the risk analysis. Mapping directly to the six question categories employed in the PIA Questionnaire, this section describes each privacy issue raised by the review, discusses the impact each privacy weakness/deficiency has on the systems and the recommendations and options available to USCIS to remove or mitigate identified risks.

### **PIA Conclusions**

In the Conclusion, USCIS will provide a summary of the PIA status and recommendations for actions to be taken with regard to the systems, prior to the new system becoming operational.

## SYSTEM IDENTIFICATION

### System Overview

These five systems are being addressed in one PIA because together they make up the current case processing system used by USCIS to process all applications that are processed electronically. Also, these systems use like information in a similar manner.

### General Description and Purpose

CLAIMS 3 and CLAIMS 4 are used by USCIS to process benefit applications, RAPS is used to adjudicate asylum applications, RNACS is used to process some naturalization applications, and MFAS is used to adjudicate petitions covered by the Immigrant Marriage Fraud Act (IMFA) of 1986. Specific details of the systems follow.

#### CLAIMS 3:

CLAIMS 3 is the primary case processing system for the adjudication of applications/petitions for all immigration benefits and services except asylum and naturalization. This 12 year-old system supports the application/petition life cycle from receipt of application to the issuance of notices and identification cards. CLAIMS 3 has two major components: (1) a client-server component operation on the service center LANs; and (2) a mainframe (M/F) component, with consolidated information compiled from periodic uploads from the client-server component(s) in the service centers. The CLAIMS 3 M/F component is accessible nation-wide to authorized USCIS representatives for online inquiry and case update. Data interfaces to other USCIS systems and to other federal agencies (e.g. Department of State) are maintained to support the full life cycle of an application/petition for benefits. In 2004, the Interim Case Management Solution (ICMS) will be added to CLAIMS 3 by web-enabling the CLAIMS 3 LAN adjudication module and providing users access over the USCIS Intranet. This will assist the District Offices to transition to the new Case Management System in the future. The primary objective of the ICMS implementation is the core District Office functionality, such as receiving applicant file information, updating case details with interview data, recording approvals/ denials, and initiating card processing of family based I-485 applications at the District Offices. Originally developed in the late 1980s, CLAIMS 3 was placed in service in the early 1990s and is now in the operations and maintenance phase of the system life cycle.

#### CLAIMS 4:

CLAIMS 4 is the primary case processing system for the adjudication of applications for naturalization (N-400). Initially developed and deployed over a 5 year period (from October 1995 to December 2000), CLAIMS 4 is now operational at 92 locations nationwide (4 Service Centers and 88 District Offices) and offers a standardized automated process for adjudicating N-400 applications. In addition, USCIS adjudicators have the ability to travel to off-site locations, such as community-based organizations, and take applications complete the examination process (interview and adjudication) for individuals who cannot travel to a USCIS office without great difficulty. CLAIMS 4 is in the Operations and Maintenance phase of the System Development Life Cycle, and the Evaluate phase of the USCIS IT Investment Management process

**RAPS:**

RAPS was developed and implemented in April 1991 to provide the capture of asylum case data, to support of case tracking, to aid in scheduling and control of case interviews, to allow for automated exchange of information with other legacy INS and external systems, to generate management and statistical reports and to generate standard forms and correspondence. On January 4, 1995, the Asylum Reform rule went into effect, streamlining adjudication of asylum applications submitted to legacy INS. Under the rule, Asylum Officers no longer prepare detailed denials as part of adjudicating asylum applications. Instead, Asylum Officers grant meritorious applications or refer applications which they do not grant to immigration judges, who in turn adjudicate the claims in either exclusion or deportation hearings. The rule also restricts employment authorization for asylum applicants whose claims either have been granted or remain pending after more than 150 days, a period that does not begin until the alien has filed a complete application and does not include delays sought or caused by the applicant. The initial impetus for development of RAPS was the implementation of a final rule, effective October 1, 1990, which provided for changes to existing asylum regulations. These new regulations provided for the establishment of a corps of Asylum Officers, fully trained in the many variations of asylum adjudications, who report directly to the Director of the Asylum Program at Headquarters Office of Refugees, Asylum, and Parole (HQRAP). The regulations also provided for procedural changes in the way claims for asylum are processed. The Asylum Officers are now based at Asylum Offices in eight cities: Miami; Chicago; Houston; San Francisco; Los Angeles; Arlington, Virginia; Newark; and New York. Until the development of RAPS, there had been no systematic way to track asylum cases, or to derive accurate statistics on the asylee population. Responses to inquiries about the numbers and nationalities of asylees who have been or whom the INS is processing necessitated manual searches and reporting by the district office staff around the country. To alleviate these problems, HQRAP requested that a centralized, automated system be developed to support the processing of currently active casework and new asylum applications. RAPS is now in the operations and maintenance phase of the system life cycle.

**RNACS:**

RNACS is a centralized Integrated Data Management System (IDMS) application accessed by users at 40 sites nationwide via cluster controllers or LAN gateways. This enables users to expedite the completion of N400, N600 and N565 naturalization application processing, facilitate the management of the naturalization program, ensure uniformity in processing, support status queries on naturalization cases nationwide, and produce integrated management and statistical reports on all naturalization casework. RNACS was developed as an interim system to provide support for naturalization processing in the period between the termination of Naturalization Casework System (NACS) and the deployment of CLAIMS 4.0. RNACS is now in the operations and maintenance phase of the system life cycle.

**MFAS:**

MFAS is a legacy mainframe-based case tracking system designed to support the adjudication of petitions covered by the Immigration Marriage Fraud Act (IMFA) of 1986. The system maintains records on eligible immigrant entrants, tracks cases, initiates and schedules interviews, generates routine correspondence, and produces management and statistical reports. MFAS is now in the operations and maintenance phase of the system life cycle.

### **Major System Components and Interconnections**

The USCIS systems interface with internal USCIS systems and external systems owned by other organizations. Internal systems include those systems that contain information about students, non-immigrants, and enforcement activities. External systems include systems that provide background information from agencies such as the FBI and CIA, and employment information from Department of Labor.

Connections to external networks, such as the Internet, dial-in and dial-out facilities and services, and dedicated connections to other government, public, or private entities shall be obtained through resources approved by the DHS CIO. External network connections shall be managed in accordance with an Interconnectivity Security Agreement (ISA) between USCIS and the non-Department entity and shall be included in the accreditation package. External network connections shall be reviewed annually by component personnel and documented in the annual information technology (IT) security assessment transmitted to the USCIS CIO and/or DHS CIO representative.

### **Information Sharing**

The legacy case management systems manage data and information associated with case processing and the delivery of benefits. The systems collect information from and share information with a number of different systems, both internal and external to USCIS. Appendix E illustrates the type of information that is shared between and among USCIS and external organizations via the legacy adjudications systems.

### **Information Sensitivity**

These systems process, store, and transmit SBU data, including investigative and intelligence data; detention and deportation, adjudications and nationality, and routine enforcement operations data; financial data; court case information; Privacy Act information; other Federal agencies' information; information regarding USCIS internal operations; and administrative information (e.g., interview results, benefit decisions, scheduled appointments, employment authorization information).

Since these systems process SBU information, they are required to have the functionality of controlled access protection (C2) level of trust as defined in Department of Defense (DOD) 5200.28, *DOD Trusted Computer Systems Evaluation Criteria*. The requirements for C2 systems include identification and authentication (I&A), discretionary access control (DAC), audit trail, and object reuse.

Table 1 shows the legacy case management system information categories and associated sensitivity levels. Sensitivity levels range from 1-3 (low to high) based on the type(s) of information processed. A Low (i.e., Level 1) sensitivity level refers to information stored, processed, or transported by the legacy case management systems, the inaccuracy, alteration, disclosure, or unavailability of which would have minimal impact on USCIS missions, functions, image, or reputation, such that the impact would place the USCIS at a significant disadvantage, or could result in loss of some tangible assets. Compromise of information of Medium (i.e., Level 2) sensitivity level would have an adverse impact and could result in loss of significant

tangible assets or resources. Compromise of information of High (i.e., Level 3) sensitivity level would have an irreparable impact such that the catastrophic result could not be repaired or set right again, or could result in the loss of major tangible assets or resources, including posing a threat to human life. The sensitivity level of the legacy case management systems is Level 3.

**Table 1. Legacy Case Management Systems Information Categories & Associated Sensitivity Levels**

<i>Information Category</i>	<i>Description</i>	<i>Sensitivity Level</i>
Investigative or Intelligence	Information related to investigations, law enforcement, and special operational activities to include information that inaccuracy of, loss of, or unauthorized alteration of could reasonably be expected to result in a loss of life.	3
Detention & Deportation, Adjudications & Nationality, and Routine Enforcement Operations	Information related to detention and deportation, adjudications data, and routine operations of enforcement groups including schedules of patrols or radio frequencies used.	2
Financial, Commercial, or Trade Secret	Information related to financial or commercial activities to include procurement, trade secrets, and proprietary information.	2
Unclassified National Security	National defense- and intelligence-related information subject to policy and procedural protection requirements under National Security Decision Directives.	2 or 3
Court Case	Information related to any current pretrial or pending cases that is not a matter of public record.	2
High or New Technology	Information related to high or new technology prohibited from disclosure to certain foreign governments, or that may require an export license.	2
Security, Threat, and Vulnerability	Information related to the USCIS security posture including automated data processing security, internal operations and control, and threat and vulnerability results.	2
Privacy Act	Any item, collection, or grouping of information about a U.S. citizen or lawfully admitted permanent resident that can be retrieved by using the person's name, Social Security number, personal registration number, or other personal identifier.	2
Other Federal Agencies	Information that belongs to another Federal agency and is not the primary responsibility of that agency. <i>Note:</i> Detailed protection requirements may be prescribed by the agency with which USCIS must comply to receive the information.	2
International	Information belonging to a foreign government. <i>Note:</i> Detailed protection requirements may be prescribed by the foreign government with which USCIS must comply to receive the information.	2
USCIS Internal Operations	Information related to routine administration and management of USCIS and not covered by any other categories.	1

## OBSERVATIONS AND RECOMMENDATIONS

Results of the PIA Questionnaire are discussed below. Observations are grouped into six sections to mirror the six questions sets in the PIA Questionnaire. General observations are discussed, followed by specific observations and recommendations. Specific observations result where the PIA Questionnaire has revealed a system privacy deficiency requiring a recommendation of action to remedy the deficiency. Please refer to Appendix D, PIA Questionnaire.

A total of five specific deficiencies requiring remediation were identified. Each has been assigned an observation number. Observations numbers were sequentially assigned; prioritization of actions is not associated with the numbering scheme.

### System Characterization

CLAIMS 3 and CLAIMS 4 are classified as a Major Applications (MA). As an MA, the system requires special management attention due to the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to, to modification of, the information in the system.

All of the systems are in the Operations and Maintenance phase of the SDLC.

### Information Sharing Practices

All of the systems are designed to collect PII from individuals and from other entities or resources. The system may also share the information it holds with other resources or entities. The information will be retrievable by the system; methodology for retrieval is yet to be determined.

### Privacy Deficiency 1

*Question 16:* When changes occur to PII held by the system or major changes to the system occur, is there a process in place to notify other resources dependent on PII contained in the system?

*Privacy Deficiency:* No process is in place for CLAIMS 3, CLAIMS 4, RNACS, RAPS or MFAS.

*Assessment:* If USCIS is a recipient agency or a source agency in a computer matching program with a nonfederal agency, a notice must be published in the Federal Register of any revisions of a matching program or system of records as defined by the Privacy Act (see Appendix B, Definitions, for the Privacy Act definitions of 'record' and 'system of records.').

*Recommendation:* BAPS will replace all of these systems.

## Privacy Deficiency 2

*Question 17:* Are processes in place for periodic review of PII contained in the system to ensure it is timely, accurate and relevant?

*Privacy Deficiency:* No processes are in place for CLAIMS 3, CLAIMS 4, RNACS, RAPS or MFAS.

*Assessment:* Under Section (e)(6) of the Privacy Act, before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2), USCIS must make reasonable efforts to ensure such records are accurate, complete, timely and relevant on each system for agency purposes. USCIS is responsible for ensuring processes are in place to verify and validate PII as directed by the Privacy Act.

*Recommendation:* BAPS will replace all of these systems.

## Web Site Host

The systems do not host an Internet and intranet Web site. The systems are not accessible by the general public. Consequently, these systems are not subject to the Federal requirements designed to protect the privacy of PII collected from individuals via the Web.

## Administrative Controls

Administrative controls are implemented to manage the security and the risk for a system and protect an organization's mission. These controls focus on policies, guidelines, and standards, which are carried out through operational procedures to prevent, detect, and recover the system.

## Privacy Deficiency 3

*Question 31:* Is there a system security plan for this system?

*Privacy Deficiency:* No, there is not a system security plan for CLAIMS 3.

*Assessment:* The Privacy Act of 1974 and OMB Circular A-130 require procedures be in place for implementing administrative, technical, and physical security controls for systems containing a system of records. Agencies should develop a plan that demonstrates security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality, and explain any planned or actual variance from NIST security guidance.

*Recommendation:* BAPS will replace all of these systems.

### Technical Controls

Technical controls are security controls configured within the system. Technical controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and secure critical and sensitive data, information, and Information Technology (IT) system functions. These controls involve system architectures; engineering disciplines; and security packages with a mix of hardware, software, and firmware.

### Privacy Deficiency 4

*Question 40:* Are the following password controls in place?

- Passwords expire after a set period of time
- Accounts are locked after a set period of inactivity
- Minimum length of passwords is eight characters
- Passwords must be a combination of uppercase, lowercase, and special characters
- Accounts are locked after a set number of incorrect attempts

*Privacy Deficiency:* None of the password controls are in place for CLAIMS 3. Only items 1, 4, and 5 are in place for MFAS. RNACS and RAPS do not have item 2.

*Assessment:* Lack of methods for ensuring password controls can lead to difficulty in protecting PII handled by the systems.

*Recommendation:* BAPS will replace all of these systems.

### Privacy Deficiency 5

*Question 41:* Is a process in place to monitor and respond to incidents?

*Privacy Deficiency:* No, no process exists or is proposed at this time for RNACS or RAPS.

*Assessment:* The benefits of an incident response capability are containing and repairing damage to a system or the information it contains from an incident and preventing future damage. It provides a way for users to report incidents and for assistance to be provided to aid recovery.

*Recommendation:* BAPS will replace these systems.

### Physical Controls

Physical controls are measures taken to protect buildings and related supporting infrastructure against threats associated with a system's physical environment. For purposes of privacy protection, appropriate controls are in place to limit physical access to these systems.

**CONCLUSION**

In general, these systems are being used in accordance with Federal, DHS and USCIS privacy requirements. In particular, the four privacy deficiencies identified in Section 5.0, Observations and Recommendations, must be addressed by USCIS as the systems are replaced by BAPS.

**APPENDIX A - ACRONYMS**

CAC	Common Access Cards
C&A	Certification and Accreditation
CCTV	Closed Circuit TV
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CLAIMS 3	Computer Linked Automated Information Management System v 3
CLAIMS 4	Computer Linked Automated Information Management System v4
CONOPS	Concept of Operations
COPPA	Children's Online Privacy Protection Act
CRIS	Customer Relationship Information System
DHS	Department of Homeland Security
DLMS	Department of Labor Manual Series
DMS	Debt Management System
DOD	Department of Defense
EID	Enforcement Integrated Database
EREM	Enforcement Removal Module
FBI	Federal Bureau of Investigation
FFMS	Federal Financial Management System
FIPS	Freedom of Information Act Information Processing System
FISMA	Federal Information Security Management Act
FTS	Fingerprint Tracking System
FOI/PA	Freedom of Information/Privacy Act
GAO	General Accounting Office
GISRA	Government Information Security Reform Act
GLBA	Gramm-Leach-Bliley Act
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
I&A	Identification and Authentication
IAFIS	Integrated Automated Fingerprint Identification System
IBIS	Interagency Border Inspection System
IDENT	Automated Biometric Fingerprint Identification System
IDS	Intrusion Detection System
PIA	

---

INS	Immigration and Naturalization Service
INSAMS	INS Allocation Management System
IP	Internet Protocol
ISRS	Image Storage and Retrieval System
IT	Information Technology
IV&V	Independent Verification and Validation
IVIS	Immigrant Visa Information System
LAN	Local Area Network
MA	Major Application
MFAS	Marriage Fraud Amendment System
NAIS	National Automated Immigration Lookout System
NCIC	National Crime Information Center
NCSC COA	National Customer Service Center Change of Address
NFTS	National File Tracking System
NIIS	Nonimmigrant Information System
NIST	National Institute of Standards and Technology
NPS	National Production System
NSA	National Security Agency
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OS	Operating System
OSHA	Occupational Safety and Health Administration
PARN	Privacy Act System of Records Notice
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PL	Public Law
POA&M	Plan of Actions and Milestones
RA	Risk Assessment
RAPS	Refugees, Asylum, and Parole System
RNACS	Reengineered Naturalization Automated Casework System
SBU	Sensitive But Unclassified
SDLC	System Development Life Cycle

---

SEVIS	Student and Exchange Visitor Information System
SIA	Service Interface Agreement
SP	Special Publication
SSP	System Security Plan
SSSP	Sensitive System Security Plan
ST&E	Security Testing and Evaluation
SWIP	Service-wide Inventory
USCIS	United States Citizenship and Immigration Services
VPN	Virtual Private Network
WAN	Wide Area Network
WATS	Washington Area Tracking System
WRAPS	Worldwide Refugee Admissions Processing System

**APPENDIX B - DEFINITIONS**

<i>Term</i>	<i>Definition</i>
Administrative Controls	Safeguards to ensure proper management and control of information and information systems. These safeguards include policy, PIAs, and certification and accreditation programs. (National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12)
Availability	A requirement intended to assure that systems work promptly and service is not denied to authorized users. (NIST SP 800-12)
Child/Children	The Children's Online Privacy Protection Act (COPPA) of 1998 defines a "child" as a person under the age of 13.
Confidentiality	A requirement that private or confidential information not be disclosed to unauthorized individuals. (NIST SP 800-12, p. 8)
Cookie	Information that a web site puts on an individual's computer so that it can remember something about the user at a later time. See also: persistent cookie, session cookie.
General Support System	An interconnected information resource under the same direct management control that shares functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from different or the same organizations. (NIST SP 800-16)
Integrity	Information that is timely, accurate, complete, and consistent. Data integrity is a requirement that information and programs are changed only in a specified and authorized manner. System integrity is a requirement that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. (NIST SP 800-12)
Major Application	An application that requires special attention to security because of the risk and magnitude of the harm resulting from loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in an MA might compromise many individual application programs and hardware, software, and telecommunications components. MAs can be either a major software application or a combination of hardware and software where the only purpose of the system is to support a specific mission-related function. For purposes of this PIA Questionnaire, an MA is expanded to include software programs capable of storing PII in file documents such as those provided in Microsoft Office (i.e., Word and Excel).
Major Change	Any change that is made to the system environment or operation of the system. The following are examples of major changes: Network, hardware, or software applications that alter the mission, operating environment, or basic vulnerabilities of the system Increase or decrease in hardware, application programs, external users, or hardware upgrades Addition of telecommunications capability Change to program logic of application systems Relocation of system to new physical environment or new organization.
Network Connected	A general support system having either modem connection capability or a network connection to a server or to one or more computers.
Persistent Cookie	A cookie that is stored on the user's hard drive and remains there until the user deletes it or it expires.
Personally Identifiable Information	Any item, collection, or grouping of information about an individual that is maintained by an agency, including education, financial transactions, medical history, and criminal or employment history. The data may also contain his or her name, other identifying number or symbol, or other identifying information unique to the individual, such as a fingerprint or a photograph. This data may be found at USCIS in the form of medical records or reports on citizens or pay and benefits information on employees.

Item	Definition
Physical Security Controls	Measures taken to protect systems buildings and related supporting infrastructure against threats associated with their physical environment. These safeguards might include protections against fire, structural collapse, plumbing leaks, physical access controls, and controls against the intercept of data. (NIST SP 800-12)
Privacy Act Systems of Records Notice (PARN)	All systems with Privacy Act information contained within them are required to publish in the Federal Register Records Notice informing the public as to, among other things, what information is contained in the system, how it is used, and how an individual may gain access to information regarding himself or herself.
Privacy Impact Assessment (PIA)	A methodology that provides IT security professionals with a process for assessing whether appropriate privacy policies, procedures, and business practices—as well as applicable administrative, technical and physical security controls—have been implemented to ensure compliance with federal privacy regulations.
Record	Any item, collection, or grouping of information about an individual identifiable to that individual and maintained by an agency. (IRS Model IT PIA)
Retrievable	A characteristic describing the ability to obtain or “pull up” a record in such a way that would allow a person to reasonably identify the subject of the record.
Risk Assessment	The process of identifying risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards to mitigate the impact. Part of Risk Management and synonymous with Risk Analysis.
Routine Use	With respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected and has been properly published in the Federal Register. [Reference Error! Reference source not found.-Error! Reference source not found.]
Sensitive System	A system that is not classified as an MA or GSS but still requires special management attention. These systems process, transmit, or store data protected under the scope of the Privacy Act of 1974, Trade Secrets Act, OMB Order on Statistical Confidentiality, OMB Statistical Policy Directive #3, the Financial Management Improvement Act of 1996, or the system’s failure would impair public confidence in USCIS.
Session Cookie	A small file, stored in temporary memory, containing information about a user that disappears when the user’s browser is closed. Unlike a persistent cookie, no file is stored on the user’s hard drive.
Stand-Alone System	A system that is neither network-connected nor connected to any other system or group of systems.
System	A system is an organized assembly of IT resources and procedures integrated and regulated by interaction or interdependence to accomplish a set of specified functions.
System of Records	A group of records under the control of any agency where information is retrieved by the name of the individual, by some identifying number or symbol, or by other identifiers assigned to the individual. (IRS Model IT PIA)
Technical Controls	Safeguards that are generally executed by the computer system. Technical safeguards include password protection, firewalls, and cryptography. (NIST SP 800-12)
Web Site	A collection of interlinked web pages (on either Internet or intranet sites) with a related topic, usually under a single domain name, which includes an intended starting file called a “home page.” From the home page, access is gained to all the other pages on the web site.

**APPENDIX C - REFERENCES**

- Children's Online Privacy Protection Act (COPPA), 15 USC § 6501 et seq.
- Computer Fraud and Abuse Act, 1984.
- Computer Matching and Privacy Act of 1988 (P.L. 100-503).
- Computer Security Act of 1987 (P.L. 100-235).
- Department of Defense (DOD) 5200.28, *DOD Trusted Computer Systems Evaluation Criteria*.
- E-Government Act of 2002, Title III, Federal Information Security Reform Act of 2002.
- Freedom of Information Act, as amended (5 U.S.C. 552).
- Government Information Security Reform Act (GISRA), October 2000.
- Health Insurance Portability and Accountability Act of 1996 (HIPPA), 29 U.S.C. § 1181 (Supp. III 1997) and implementing regulations. Privacy Rule, 67 FR 14775.
- Office of Management and Budget Circular A-130, Management of Federal Information Resources.
- OMB Circular A-11 (Exhibit 300).
- OMB Memorandum No. M-99-18 "Privacy Policies on Federal Web Sites," June 2, 1999.
- OMB Memorandum No. M-00-13 "Privacy Policies and Data Collection on Federal Web Sites," June 22, 2000.
- OMB Memorandum for the Heads of Executive Departments and Agencies, Subject: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 30, 2003).
- Privacy Act of 1974, 5 U.S.C. 552a, as amended.
- Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.).

**APPENDIX D – PIA QUESTIONNAIRE – CLAIMS 3**

**NOTE:** Based on current privacy regulation and guidance, the PIA should be performed on the production environment. For those systems that have test and development environments, those environments may or may not warrant their own Privacy Impact Assessment (PIA). The test and development environments generally do not necessitate a separate PIA, however, the assessor may need to consult information technology (IT) system policy guidance and/or its system security officer and/or the Office of the Chief Information Officer (OCIO) to confirm such decisions. For those systems that have performed risk assessments and defined systems boundaries and scope, the system characterization will also be the same for both the risk assessment and this PIA. PIAs performed on the production environment will require conducting another PIA at intervals stipulated by the security handbook and when significant changes occur to the system.

The PIA attempts to determine what kind of personal information is contained within a system, what is done with that information and how that information is protected. It lists primary requirements for systems containing personal information as defined in context with privacy laws, regulations, and guidance. It is intended to be used as a tool to provide a starting point for meeting certain requirements. However, users should be informed that privacy laws and decisions have updated for amendments of the Privacy Act statute. The Privacy Officer can answer questions related to technical and physical controls of a system and in all cases, keep a record of all questionnaire responses.

**System Name:** United States Citizenship and Immigration Services (USCIS)  
Computer Linked Automated Information Management System  
(CLAIMS 3)

**System Environment** (production, test, development, or other. If other, please explain): Production

**System Location** (entity/contractor name of site, building, room, city, and state): N/A

**Activity/Purpose of System:** To track, process and report on applications for immigration benefits.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>System Characterization</b>					
1	<p><b>Does USCIS own the system?</b></p> <p>Note: If no, identify the system owner in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Owner: (b)(6)
2	<p><b>Does USCIS operate the system?</b></p> <p>Note: If no, identify the system operator in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3	<p><b>Identify in the Comments column the life-cycle phase of this system.</b></p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Initiation <input type="checkbox"/> Develop/Acquisition <input type="checkbox"/> Implementation <input checked="" type="checkbox"/> Operations/Maintenance <input type="checkbox"/> Disposal
4	<p><b>Is the system a stand-alone system (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire)?</b></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	<p><b>Is the system network-connected (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire)?</b></p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
6	<p><b>Is the system a General Support System (GSS), Major Application (MA) or sensitive system (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire)?</b></p> <p>Note: If yes, identify whether the system is a GSS, MA or sensitive system in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Sensitive But Unclassified

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>System Characterization</b>					
7	<p><b>Does the system contain PII within any database(s), record(s), file(s) or document(s)?</b></p> <p>Note: If yes, check all that apply in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If the system contains no records with any data elements listed in the comments section, the system is not subject to federal privacy laws or regulations such as the <i>Privacy Act of 1974</i>. Questions 8-18 may be marked with an "N/A."</p> <p>If data elements relating to persons who are either United States Citizens or Lawful Permanent Residents are checked under the personal information category in the comments column, then the <i>Privacy Act of 1974</i> is invoked. Agencies must meet all requirements of the Privacy Act listed under <i>5 U.S.C. 552a.(4)</i> as amended, listed under "Records Maintained On Individuals."</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then the <i>HIPAA Privacy Rule 67 FR 14775</i> may be invoked. Agencies should review this rule to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then the <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p><b>Personal Information:</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Name</li> <li><input checked="" type="checkbox"/> Date of Birth</li> <li><input checked="" type="checkbox"/> Social Security Number (or other number originated by a government that specifically identifies an individual)</li> <li><input checked="" type="checkbox"/> Photographic Identifiers (e.g., photograph image, x-rays, and video)</li> <li><input checked="" type="checkbox"/> Driver's License</li> <li><input checked="" type="checkbox"/> Biometric Identifiers (e.g., fingerprint and voiceprint)</li> <li><input checked="" type="checkbox"/> Mother's Maiden Name</li> <li><input type="checkbox"/> Vehicle Identifiers (e.g., license plates)</li> <li><input checked="" type="checkbox"/> Mailing Address</li> <li><input checked="" type="checkbox"/> Phone Numbers (e.g., phone, fax, and cell)</li> <li><input type="checkbox"/> Medical Records Numbers</li> <li><input type="checkbox"/> Medical Notes</li> <li><input checked="" type="checkbox"/> Financial Account Information and/or Numbers (e.g., checking account number and PINs)</li> <li><input checked="" type="checkbox"/> Certificates (e.g., birth, death, and marriage)</li> <li><input checked="" type="checkbox"/> Legal Documents or Notes (e.g., divorce decree, criminal records, or other)</li> <li><input type="checkbox"/> Device Identifiers (e.g., pacemaker, hearing aid, or other)</li> <li><input type="checkbox"/> Web URLs</li> <li><input type="checkbox"/> Email Address</li> <li><input type="checkbox"/> Education Records</li> <li><input checked="" type="checkbox"/> Other: Alien Number (A-Number)</li> </ul>

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>System Characterization</b>					
8	<p><b>Has a Privacy Act Systems of Records Notice (PARN) been published in the Federal Register?</b></p> <p><b>Remediation Guidance:</b> If no, and the system meets the definition of a System of Records, then the <i>Privacy Act of 1974</i> requirements are invoked. Agencies must develop a PARN and publish the notice in the Federal Register with appropriate specifications listed in <i>5 U.S.C. Section 552a</i> as amended.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>Federal Register Notice published 10/17/02.</p> <p>67FR64132</p>
9	<p><b>Have major changes (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire) to the system been made since publication of the PARN?</b></p> <p><b>Remediation Guidance:</b> If yes, then the <i>Privacy Act of 1974</i> requires that agencies publish in the Federal Register a notice of any, and all revisions to the existence and character of the system of records with appropriate specifications listed in <i>5 U.S.C. Section 552a</i> as amended.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
10	<p><b>Does the PARN address all required categories of information?</b></p> <p>Note: Check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, then the notice specifying the existence of the system of records will include all criteria listed in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> System Name</li> <li><input type="checkbox"/> Security Classification</li> <li><input checked="" type="checkbox"/> System Location</li> <li><input checked="" type="checkbox"/> Categories of Individuals Covered by the System</li> <li><input checked="" type="checkbox"/> Categories of Records in the System</li> <li><input checked="" type="checkbox"/> Authority of Maintenance of the System</li> <li><input checked="" type="checkbox"/> Purpose</li> <li><input checked="" type="checkbox"/> Routine Uses of Records Maintained in the System</li> <li><input type="checkbox"/> Disclosure to Consumer Reporting Agencies</li> <li><input checked="" type="checkbox"/> Policies and Practices for Storing, Retrieving, Accessing, Retaining and Disposing of Records</li> <li><input checked="" type="checkbox"/> System Manager(s) and Address</li> <li><input checked="" type="checkbox"/> Notification Procedure</li> <li><input checked="" type="checkbox"/> Record Access Procedure</li> <li><input checked="" type="checkbox"/> Contesting Record Procedure</li> <li><input checked="" type="checkbox"/> Record Source Categories</li> <li><input checked="" type="checkbox"/> Systems Exempted From Certain Provisions of the Act</li> </ul>

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
11	<p><b>Does the system collect PII from individuals?</b></p> <p>Note: If yes, identify the PII the system collects directly from individuals in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> Each agency maintaining system of records is required to collect information to the greatest extent practicable directly from the individual when information may result in adverse determinations about an individual's rights, benefits, and privileges under federal programs.</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then <i>HIPAA Privacy Rule 67 FR 14775</i> may be invoked. Agencies should review these rules to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p><b>Personal Information:</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Alien Registration Number</li> <li><input checked="" type="checkbox"/> Name</li> <li><input checked="" type="checkbox"/> Date of Birth</li> <li><input checked="" type="checkbox"/> Social Security Number (or other number originated by a government that specifically identifies an individual)</li> <li><input checked="" type="checkbox"/> Photographic Identifiers (e.g., photograph image, x-rays, and video)</li> <li><input type="checkbox"/> Driver's License</li> <li><input checked="" type="checkbox"/> Biometric Identifiers (e.g., fingerprint and voiceprint)</li> <li><input checked="" type="checkbox"/> Mother's Maiden Name</li> <li><input type="checkbox"/> Vehicle Identifiers (e.g., license plates)</li> <li><input checked="" type="checkbox"/> Mailing Address</li> <li><input checked="" type="checkbox"/> Phone Numbers (e.g., phone, fax, and cell)</li> <li><input type="checkbox"/> Medical Records Numbers</li> <li><input type="checkbox"/> Medical Notes</li> <li><input checked="" type="checkbox"/> Financial Account Information and/or Numbers (e.g., checking account number and PINs)</li> <li><input checked="" type="checkbox"/> Certificates (e.g., birth, death, and marriage)</li> <li><input checked="" type="checkbox"/> Legal Documents or Notes (e.g., divorce decree, criminal records, or other)</li> <li><input type="checkbox"/> Device Identifiers (e.g., pacemaker, hearing aid, or other)</li> <li><input type="checkbox"/> Web URLs</li> <li><input type="checkbox"/> E-mail Address</li> <li><input type="checkbox"/> Education Records</li> <li><input type="checkbox"/> Other: _____</li> </ul>

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
12	<p><b>Does the system collect PII from other sources (e.g., databases, websites, etc.)?</b></p> <p>Note: If yes, specify the source(s) and PII collected in the Comments column.</p> <p><b>Remediation Guidance:</b> If yes, then each agency is required to maintain records on systems that are used for making determinations about an individual with accuracy, relevance, timeliness, and completeness as reasonably necessary to assure fairness to the individual. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the <i>Privacy Act of 1974</i>.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
13	<p><b>Does the system populate data for other resources (i.e., do databases, web sites, or other resources rely on this system's data)?</b></p> <p>Note: If yes, specify resource(s) and purpose for each instance in the Comments column.</p> <p><b>Remediation Guidance:</b> If yes, then section (e) (6) of the <i>Privacy Act of 1974</i> is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, the agency must make reasonable efforts to assure that such records are accurate, complete, timely, and relevant on each system for agency purposes. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the Act.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
14	<p><b>Does the system <i>share</i> PII with internal or external parties of USCIS?</b></p> <p>Note: If yes, identify in the Comments column which data elements are shared. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If yes, then section (e) (6) of the <i>Privacy Act of 1974</i> is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, agencies must make reasonable efforts to ensure that such records are accurate, complete, timely, and relevant on each system for agency purposes. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the Act.</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then <i>HIPAA Privacy Rule, 67 FR 14775</i> may be invoked. Agencies should review these rules to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
15	<p><b>Are records on the system retrievable?</b></p> <p>Note: If yes, specify in the Comments column what method is used in retrieving the records (i.e., using a record number, name, social security number, or other data element or record locator methodology). If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If yes, then a system of records in which information relating to a United States citizen or Lawful Permanent Resident is retrieved using one or more of an individual's "identifying information" invokes <i>Privacy Act of 1974</i> requirements. All requirements under <i>5 U.S.C. of Section 552a</i> as amended must be met by an agency for this system.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
16	<p><b>Is there a notification process in place when changes occur (i.e., revisions to PII or when the system encounters a major change or is replaced) for alerting other resources dependent upon PII contained on this system?</b></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
17	<p><b>Are processes in place for periodic review of PII contained in the system to ensure it is timely, accurate, and relevant?</b></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
18	<p><b>Are rules of conduct in place for access to PII on the system?</b></p> <p>Note: If yes, identify in the Comments column all users with access to PII on the system, and for what purposes they use the PII.</p> <p><b>Remediation Guidance:</b> If no, then Section (e)(9-10) of the <i>Privacy Act of 1974</i> is invoked to the extent that the system contains information relating to United States citizens or Lawful Permanent Residents. The Act requires rules of conduct for persons involved in the design, development, operations, or maintenance of a system's PII.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p><input checked="" type="checkbox"/> Users  <input checked="" type="checkbox"/> Administrators  <input checked="" type="checkbox"/> Developers  <input checked="" type="checkbox"/> Contractors</p> <p>For what purposes:  <input type="checkbox"/> _____  <input type="checkbox"/> _____  <input type="checkbox"/> _____  <input type="checkbox"/> _____</p> <p>All users listed will be subject to USCIS and Rules of Behavior</p>
19	<p><b>Does the system host a web site either as an Internet, an intranet, or both?</b></p> <p>Note: If yes, identify what type of site in the Comments column.</p> <p><b>Note: If no, check N/A for all subsequent questions in the "Web Site Host Question Sets" section and answer questions starting with the "Administrative Controls" section beginning with Question #28.</b></p> <p><b>Remediation Guidance:</b> If yes, then <i>OMB M-99-18</i> is invoked requiring that for every federal, public web site agencies include a privacy policy statement, even if the site does <i>not</i> collect any information and does not create a Privacy Act record.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>Intranet site for National Benefits Center access</p>

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
20	<p><b>Is the web site accessible by the public or other entities (i.e., contractors, third party administrators, state, or local agencies, etc.)?</b></p> <p><b>Remediation Guidance:</b> If yes, then <i>OMB M-99-18</i> is invoked. Agencies must post privacy policies on their principal web sites, any known major entry points, and any web page where substantial personal information is collected from the public. The privacy policy must state what information is being collected, why it is being collected, and how the agency will use the information. Privacy policies must be clearly labeled and easily accessed when an individual visits a web site.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	See Question 19 above.
21	<p><b>Is a privacy policy statement posted on the web site?</b></p> <p><b>Remediation Guidance:</b> If no, then <i>OMB M-99-18</i> is invoked. Agencies must post privacy policies on their principal web sites, any known major entry points, as well as any web pages where substantial personal information is collected from the public. The privacy policy must state what information is being collected, why it is being collected, and how the agency will use the information. Privacy policies must be clearly labeled and easily accessed when an individual visits a web site.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.
22	<p><b>Are web links posted anywhere on the web site?</b></p> <p><b>Remediation Guidance:</b> If no, then <i>OMB M-99-18</i> is invoked. Agencies must post privacy policies on their principal web sites, any known major entry points, as well as any web pages where substantial personal information is collected from the public. The privacy policy must state what information is being collected, why it is being collected, and how the agency will use the information. Privacy policies must be clearly labeled and easily accessed when an individual visits a web site.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
23	<p><b>Are cookies present on the web site?</b></p> <p>Note: If yes, identify types of cookies in the Comments column.</p> <p><b>Remediation Guidance:</b> If yes, persistent cookies are prohibited. Alternatively, session cookies are allowed as long as use of session cookies are indicated in the privacy policy statement, and the agency is able to demonstrate a valid need for use of these session cookies. Cookies will not knowingly be transferred to third parties unless explained in the Privacy and Security Statement.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.
24	<p><b>Does the web site have any information or pages directed at children?</b></p> <p><b>Remediation Guidance:</b> If yes, then the <i>Children's Online Privacy Protection Act (COPPA)</i>, <i>OMB M-00-13</i>, and <i>DLMS 9 Chapter 1500</i> are all invoked. Agency systems hosting web sites are mandated by OMB to comply with COPPA. This law places restrictions on the collection and use of information on any web site or online service directed to children and requires parental consent before any such collection and provides the parent with the right to see what is collected about his/her child and to restrict dissemination or use or further collection of any information about the child.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
25	<p><b>Does the web site collect PII from individuals?</b></p> <p>Note: If yes, identify what PII the system collects in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b>                      If yes, and data elements relating to United States citizens or Lawful Permanent Residents are checked under both the Identifier and Personal Information categories, then the <i>Privacy Act of 1974</i> is invoked. Agencies must meet all requirements of the Privacy Act listed under <i>5 U.S.C. 552a.(4)</i> as amended listed under "Records Maintained On Individuals."</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then the <i>HIPAA Privacy Rule, 67 FR 14775</i> may be invoked. Agencies should review this rule to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then the <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
26	<p><b>Does the web site <i>share</i> PII with internal or external parties of the Department?</b>                      Note: If yes, specify with whom and for what purposes, and identify the data elements in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b>                      If yes and the information relates to United States citizens or Lawful Permanent Residents, then section (e) (6) of the Privacy Act is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, agencies must make reasonable efforts to ensure that such records are accurate, complete, timely, and relevant on each system for agency purposes. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the Act.</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then <i>HIPAA Privacy Rule, 67 FR 14775</i> may be invoked. Agencies should review these rules to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then <i>Gramm-Leach-Bliley Act (GLBA) of 1999 Pub. Law No. 106-102, 113 Stat. 1338 (1999)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	See Question 19 above.
27	<p><b>Are rules of conduct in place for access to PII on the website?</b></p> <p>Note: If yes, identify in the Comments column all categories of users with access to PII on the system, and for what purposes the PII is used.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Administrative Controls</b>					
<p><b>Note:</b> This PIA Guide uses the terms “Administrative,” “Technical,” and “Physical” to refer to security control questions—terms that are used in several federal privacy laws when referencing security requirements. USCIS recognizes the slight difference in terminology used in this guide from those that are used in other documents such as the <i>National Institute of Standards and Technology (NIST) SP 800-26, Security Self-Assessment Guide for Information Technology Systems</i>.</p>					
28	<p><b>Has the system been authorized to process information?</b></p> <p><b>Remediation Guidance:</b> If no, then the system may be required as directed by <i>OMB Circular A-130</i> to complete an accreditation for each system. Agencies should engage in an assessment process that ensures technical security features are built into the life cycle of a system.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
29	<p><b>Have there been major changes (as defined in Appendix A, “Glossary of Terms” of the PIA Questionnaire) to the system since it was last certified and accredited?</b></p> <p><b>Remediation Guidance:</b> If yes, then agencies are required by <i>OMB Circular A-130</i> to complete an update of the certification and accreditation for each system that has been modified. Agencies should engage in an assessment process that ensures existing technical security features are appropriate to the modified system.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
30	<p><b>Are security controls routinely reviewed?</b></p> <p><b>Remediation Guidance:</b> Security controls need to be routinely reviewed to ensure sustained effectiveness even when no changes to the system have occurred. <i>OMB Circular A-130</i> stipulates a system’s security controls should be reviewed “when significant modifications are made to a system, but at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system.”</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Administrative Controls</b>					
31	<p><b>Is there a system security plan for this system?</b></p> <p><b>Remediation Guidance:</b>                      The <i>Privacy Act of 1974</i> and <i>OMB Circular A-130</i> require procedures be in-place for implementing administrative, technical, and physical security controls for systems containing a system of records. Agencies should develop a plan that demonstrates security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from NIST security guidance.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	CLAIMS 3 is a distributed client/server system which is not managed by any one entity.
32	<p><b>Is there a contingency (or backup) plan for the system?</b></p> <p><b>Remediation Guidance:</b>                      The <i>Privacy Act of 1974</i> and <i>OMB Circular A-130</i> require procedures be in place for implementing a contingency plan for systems containing a system of records. Agencies should develop a plan that demonstrates contingency security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from NIST security guidance.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
33	<p><b>Are files backed up regularly?</b></p> <p><b>Remediation Guidance:</b>  <i>OMB Circular A-130</i> requires procedures be in place for protecting data on systems in the event the system and the information it contains is attacked or rendered unavailable. Agencies should devise a method for backing up information contained on the system at regular intervals.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Daily backups are performed.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Administrative Controls</b>					
34	<p><b>Are the backup files stored offsite?</b></p> <p><b>Remediation Guidance:</b> OMB Circular A-130 requires procedures be in place for protecting data on systems in the event the system and the information it contains is attacked or rendered unavailable. Agencies should identify an alternative site for housing backup files.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
35	<p><b>Are there user manuals for the system?</b></p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
36	<p><b>Have personnel using the system been trained and made aware of their responsibilities for protecting personal information being collected and maintained?</b></p> <p><b>Remediation Guidance:</b> If no, OMB Circular A-130 requires that each agency ensure the security of information contained on each system to include training of users and employees of security controls in place. Agencies should provide users with training of their roles and responsibilities for protecting PII collected and maintained on the system.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
37	<p><b>Who will have access to the PII on the system?</b></p> <p>Note: Check all that apply in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Users <input checked="" type="checkbox"/> Administrators <input checked="" type="checkbox"/> Developers <input checked="" type="checkbox"/> Contractors
38	<p><b>Are methods in place to ensure least privilege (e.g., "need to know" and accountability)?</b></p> <p>Note: If yes, please specify method(s) in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Technical Controls</b>					
39	<p><b>Are technical controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system?</b></p> <p>Note: If yes, check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, <i>OMB Circular A-130</i> requires that each agency ensure the security of information contained on each system by implementing technical security controls. Agencies should devise administrative, technical, and physical controls for each system to protect the PII it contains.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>USCIS has established technical control requirements including the following controls:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> User ID</li> <li><input checked="" type="checkbox"/> Passwords</li> <li><input checked="" type="checkbox"/> Firewall</li> <li><input type="checkbox"/> Virtual Private Network (VPN)</li> <li><input type="checkbox"/> Encryption</li> <li><input type="checkbox"/> Intrusion Detection System (IDS)</li> <li><input type="checkbox"/> Common Access Cards (CAC)</li> <li><input type="checkbox"/> Smart Cards</li> <li><input type="checkbox"/> Biometrics</li> <li><input type="checkbox"/> Public Key Infrastructure (PKI)</li> </ul>
40	<p><b>Are the following password controls in place?</b></p> <p>Note: Check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, <i>OMB Circular A-130</i> requires that each agency ensure the security of information contained on each system. Agencies should implement one or more of the password controls for each system to protect the PII it contains.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Passwords expire after a set period of time.</li> <li><input type="checkbox"/> Accounts are locked after a set period of inactivity.</li> <li><input type="checkbox"/> Minimum length of passwords is eight characters.</li> <li><input type="checkbox"/> Passwords must be a combination of uppercase, lowercase, and special characters.</li> <li><input type="checkbox"/> Accounts are locked after a set number of incorrect attempts.</li> </ul> <p>USCIS has established password management security requirements</p>
41	<p><b>Is a process in place to monitor and respond to incidents?</b></p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Physical Controls</b>					
42	<p><b>Are physical access controls in place?</b></p> <p>Note: If yes, check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, <i>OMB Circular A-130</i> requires that each agency ensure the security of information contained on each system by implementing technical security controls. Agencies should devise administrative, technical, and physical controls for each system to protect the PII it contains.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>USCIS controls include:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Guards</li> <li><input checked="" type="checkbox"/> Identification Badges</li> <li><input checked="" type="checkbox"/> Key Cards</li> <li><input type="checkbox"/> Cipher Locks</li> <li><input type="checkbox"/> Biometrics</li> <li><input type="checkbox"/> Closed Circuit TV (CCTV)</li> <li><input type="checkbox"/> Other _____</li> <li><input type="checkbox"/> Other _____</li> <li><input type="checkbox"/> Other _____</li> </ul>

**APPENDIX D – PIA QUESTIONNAIRE – CLAIMS 4**

**NOTE:** Based on current privacy regulation and guidance, the PIA should be performed on the production environment. For those systems that have test and development environments, these environments may or may not warrant their own Privacy Impact Assessment (PIA). The test and development environments generally do not necessitate a separate PIA, however, the assessor may need to consult information technology (IT) system policy guidance or other security officer and/or the chief of the Information Operations Office (CIO) for clarification in such decisions. For those systems that have performed risk assessments and defined system boundaries and scope, the system characterization will likely be the same for a privacy risk assessment and PIA. PIA's performed at the initial end of the system development life cycle will require conducting another PIA at intervals stipulated by the security handbook and when significant changes occur to the system.

The PIA will assess system risks which include personal information contained within systems which is dependent on the information and the way that information is protected. While there are many regulations, systems, and all personal information, a system may be exempt from privacy law by exemption and/or guidance. The remediation guidelines provided at the end of this starting point form contain certain requirements. However, as is noted in the remediation guidelines, a system may not be exempt from the provisions of the Privacy Act. The CIO can answer the questions related to the exemption, and the physical controls of the system and the measures to the clarification of questionnaire questions.

**System Name:** United States Citizenship and Immigration Services (USCIS)  
Computer Linked Automated Information Management System  
(CLAIMS 4)

**System Environment** (production, test, development, or other. If other, please explain): Production

**System Location** (entity/contractor name of site, building, room, city, and state): N/A

**Activity/Purpose of System:** To track, process and report on applications for immigration benefits.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>System Characterization</b>					
1	<p><b>Does USCIS own the system?</b></p> <p>Note: If no, identify the system owner in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Owner: <b>b(6)</b>
2	<p><b>Does USCIS operate the system?</b></p> <p>Note: If no, identify the system operator in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3	<p><b>Identify in the Comments column the life-cycle phase of this system.</b></p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Initiation <input type="checkbox"/> Develop/Acquisition <input type="checkbox"/> Implementation <input checked="" type="checkbox"/> Operations/Maintenance <input type="checkbox"/> Disposal
4	<p><b>Is the system a stand-alone system (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire)?</b></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	<p><b>Is the system network-connected (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire)?</b></p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
6	<p><b>Is the system a General Support System (GSS), Major Application (MA) or sensitive system (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire)?</b></p> <p>Note: If yes, identify whether the system is a GSS, MA or sensitive system in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Sensitive But Unclassified

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>System Characterization</b>					
7	<p><b>Does the system contain PII within any database(s), record(s), file(s) or document(s)?</b></p> <p>Note: If yes, check all that apply in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If the system contains no records with any data elements listed in the comments section, the system is not subject to federal privacy laws or regulations such as the <i>Privacy Act of 1974</i>. Questions 8-18 may be marked with an "N/A."</p> <p>If data elements relating to persons who are either United States Citizens or Lawful Permanent Residents are checked under the personal information category in the comments column, then the <i>Privacy Act of 1974</i> is invoked. Agencies must meet all requirements of the Privacy Act listed under 5 U.S.C. 552a.(4) as amended, listed under "Records Maintained On Individuals."</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then the <i>HIPAA Privacy Rule 67 FR 14775</i> may be invoked. Agencies should review this rule to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then the <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p><b>Personal Information:</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Name</li> <li><input checked="" type="checkbox"/> Date of Birth</li> <li><input checked="" type="checkbox"/> Social Security Number (or other number originated by a government that specifically identifies an individual)</li> <li><input checked="" type="checkbox"/> Photographic Identifiers (e.g., photograph image, x-rays, and video)</li> <li><input checked="" type="checkbox"/> Driver's License</li> <li><input checked="" type="checkbox"/> Biometric Identifiers (e.g., fingerprint and voiceprint)</li> <li><input checked="" type="checkbox"/> Mother's Maiden Name</li> <li><input type="checkbox"/> Vehicle Identifiers (e.g., license plates)</li> <li><input checked="" type="checkbox"/> Mailing Address</li> <li><input checked="" type="checkbox"/> Phone Numbers (e.g., phone, fax, and cell)</li> <li><input type="checkbox"/> Medical Records Numbers</li> <li><input type="checkbox"/> Medical Notes</li> <li><input checked="" type="checkbox"/> Financial Account Information and/or Numbers (e.g., checking account number and PINs)</li> <li><input checked="" type="checkbox"/> Certificates (e.g., birth, death, and marriage)</li> <li><input checked="" type="checkbox"/> Legal Documents or Notes (e.g., divorce decree, criminal records, or other)</li> <li><input type="checkbox"/> Device Identifiers (e.g., pacemaker, hearing aid, or other)</li> <li><input type="checkbox"/> Web URLs</li> <li><input type="checkbox"/> Email Address</li> <li><input type="checkbox"/> Education Records</li> <li><input checked="" type="checkbox"/> Other: Alien Number (A-Number)</li> </ul>

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>System Characterization</b>					
8	<p><b>Has a Privacy Act Systems of Records Notice (PARN) been published in the Federal Register?</b></p> <p><b>Remediation Guidance:</b> If no, and the system meets the definition of a System of Records, then the <i>Privacy Act of 1974</i> requirements are invoked. Agencies must develop a PARN and publish the notice in the Federal Register with appropriate specifications listed in <i>5 U.S.C. Section 552a</i> as amended.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>Federal Register Notice published 10/17/02.</p> <p>67FR64132</p>
9	<p><b>Have major changes (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire) to the system been made since publication of the PARN?</b></p> <p><b>Remediation Guidance:</b> If yes, then the <i>Privacy Act of 1974</i> requires that agencies publish in the Federal Register a notice of any, and all revisions to the existence and character of the system of records with appropriate specifications listed in <i>5 U.S.C. Section 552a</i> as amended.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
10	<p><b>Does the PARN address all required categories of information?</b></p> <p>Note: Check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, then the notice specifying the existence of the system of records will include all criteria listed in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> System Name <input type="checkbox"/> Security Classification <input checked="" type="checkbox"/> System Location <input checked="" type="checkbox"/> Categories of Individuals Covered by the System <input checked="" type="checkbox"/> Categories of Records in the System <input checked="" type="checkbox"/> Authority of Maintenance of the System <input checked="" type="checkbox"/> Purpose <input checked="" type="checkbox"/> Routine Uses of Records Maintained in the System <input type="checkbox"/> Disclosure to Consumer Reporting Agencies <input checked="" type="checkbox"/> Policies and Practices for Storing, Retrieving, Accessing, Retaining and Disposing of Records <input checked="" type="checkbox"/> System Manager(s) and Address <input checked="" type="checkbox"/> Notification Procedure <input checked="" type="checkbox"/> Record Access Procedure <input checked="" type="checkbox"/> Contesting Record Procedure <input checked="" type="checkbox"/> Record Source Categories <input checked="" type="checkbox"/> Systems Exempted From Certain Provisions of the Act

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
11	<p><b>Does the system collect PII from individuals?</b></p> <p>Note: If yes, identify the PII the system collects directly from individuals in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> Each agency maintaining system of records is required to collect information to the greatest extent practicable directly from the individual when information may result in adverse determinations about an individual's rights, benefits, and privileges under federal programs.</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then <i>HIPAA Privacy Rule 67 FR 14775</i> may be invoked. Agencies should review these rules to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p><b>Personal Information:</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Alien Registration Number</li> <li><input checked="" type="checkbox"/> Name</li> <li><input checked="" type="checkbox"/> Date of Birth</li> <li><input checked="" type="checkbox"/> Social Security Number (or other number originated by a government that specifically identifies an individual)</li> <li><input checked="" type="checkbox"/> Photographic Identifiers (e.g., photograph image, x-rays, and video)</li> <li><input type="checkbox"/> Driver's License</li> <li><input checked="" type="checkbox"/> Biometric Identifiers (e.g., fingerprint and voiceprint)</li> <li><input checked="" type="checkbox"/> Mother's Maiden Name</li> <li><input type="checkbox"/> Vehicle Identifiers (e.g., license plates)</li> <li><input checked="" type="checkbox"/> Mailing Address</li> <li><input checked="" type="checkbox"/> Phone Numbers (e.g., phone, fax, and cell)</li> <li><input type="checkbox"/> Medical Records Numbers</li> <li><input type="checkbox"/> Medical Notes</li> <li><input checked="" type="checkbox"/> Financial Account Information and/or Numbers (e.g., checking account number and PINs)</li> <li><input checked="" type="checkbox"/> Certificates (e.g., birth, death, and marriage)</li> <li><input checked="" type="checkbox"/> Legal Documents or Notes (e.g., divorce decree, criminal records, or other)</li> <li><input type="checkbox"/> Device Identifiers (e.g., pacemaker, hearing aid, or other)</li> <li><input type="checkbox"/> Web URLs</li> <li><input type="checkbox"/> E-mail Address</li> <li><input type="checkbox"/> Education Records</li> <li><input type="checkbox"/> Other: _____</li> </ul>

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
12	<p><b>Does the system collect PII from other sources (e.g., databases, websites, etc.)?</b></p> <p>Note: If yes, specify the source(s) and PII collected in the Comments column.</p> <p><b>Remediation Guidance:</b> If yes, then each agency is required to maintain records on systems that are used for making determinations about an individual with accuracy, relevance, timeliness, and completeness as reasonably necessary to assure fairness to the individual. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the <i>Privacy Act of 1974</i>.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>SSA, IRS, DOS, DOL</p> <p><input checked="" type="checkbox"/> Name  <input checked="" type="checkbox"/> Date of Birth  <input checked="" type="checkbox"/> Social Security Number (or other number originated by a government that specifically identifies an individual)  <input checked="" type="checkbox"/> Legal Documents or Notes (e.g., divorce decree, criminal records, or other)</p>
13	<p><b>Does the system populate data for other resources (i.e., do databases, web sites, or other resources rely on this system's data)?</b></p> <p>Note: If yes, specify resource(s) and purpose for each instance in the Comments column.</p> <p><b>Remediation Guidance:</b> If yes, then section (e) (6) of the <i>Privacy Act of 1974</i> is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, the agency must make reasonable efforts to assure that such records are accurate, complete, timely, and relevant on each system for agency purposes. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the Act.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p><input checked="" type="checkbox"/> Name  <input checked="" type="checkbox"/> Date of Birth  <input checked="" type="checkbox"/> Social Security Number (or other number originated by a government that specifically identifies an individual)  <input checked="" type="checkbox"/> Legal Documents or Notes (e.g., divorce decree, criminal records, or other)</p>

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
14	<p><b>Does the system <i>share</i> PII with internal or external parties of USCIS?</b></p> <p>Note: If yes, identify in the Comments column which data elements are shared. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If yes, then section (e) (6) of the <i>Privacy Act of 1974</i> is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, agencies must make reasonable efforts to ensure that such records are accurate, complete, timely, and relevant on each system for agency purposes. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the Act.</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then <i>HIPAA Privacy Rule, 67 FR 14775</i> may be invoked. Agencies should review these rules to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Name <input checked="" type="checkbox"/> Date of Birth <input checked="" type="checkbox"/> Social Security Number (or other number originated by a government that specifically identifies an individual) <input checked="" type="checkbox"/> Legal Documents or Notes (e.g., divorce decree, criminal records, or other)

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
15	<p><b>Are records on the system retrievable?</b></p> <p>Note: If yes, specify in the Comments column what method is used in retrieving the records (i.e., using a record number, name, social security number, or other data element or record locator methodology). If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If yes, then a system of records in which information relating to a United States citizen or Lawful Permanent Resident is retrieved using one or more of an individual's "identifying information" invokes <i>Privacy Act of 1974</i> requirements. All requirements under <i>5 U.S.C. of Section 552a</i> as amended must be met by an agency for this system.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
16	<p><b>Is there a notification process in place when changes occur (i.e., revisions to PII or when the system encounters a major change or is replaced) for alerting other resources dependent upon PII contained on this system?</b></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
17	<p><b>Are processes in place for periodic review of PII contained in the system to ensure it is timely, accurate, and relevant?</b></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
18	<p><b>Are rules of conduct in place for access to PII on the system?</b></p> <p>Note: If yes, identify in the Comments column all users with access to PII on the system, and for what purposes they use the PII.</p> <p><b>Remediation Guidance:</b> If no, then Section (e)(9-10) of the <i>Privacy Act of 1974</i> is invoked to the extent that the system contains information relating to United States citizens or Lawful Permanent Residents. The Act requires rules of conduct for persons involved in the design, development, operations, or maintenance of a system's PII.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p><input checked="" type="checkbox"/> Users  <input checked="" type="checkbox"/> Administrators  <input checked="" type="checkbox"/> Developers  <input checked="" type="checkbox"/> Contractors</p> <p>For what purposes:  <input type="checkbox"/> _____  <input type="checkbox"/> _____  <input type="checkbox"/> _____  <input type="checkbox"/> _____  <input type="checkbox"/> _____</p> <p>All users listed will be subject to USCIS and Rules of Behavior</p>
19	<p><b>Does the system host a web site either as an Internet, an intranet, or both?</b></p> <p>Note: If yes, identify what type of site in the Comments column.</p> <p>Note: If no, check N/A for all subsequent questions in the "Web Site Host Question Sets" section and answer questions starting with the "Administrative Controls" section beginning with Question #28.</p> <p><b>Remediation Guidance:</b> If yes, then <i>OMB M-99-18</i> is invoked requiring that for every federal, public web site agencies include a privacy policy statement, even if the site does not collect any information and does not create a Privacy Act record.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
20	<p><b>Is the web site accessible by the public or other entities (i.e., contractors, third party administrators, state, or local agencies, etc.)?</b></p> <p><b>Remediation Guidance:</b> If yes, then <i>OMB M-99-18</i> is invoked. Agencies must post privacy policies on their principal web sites, any known major entry points, and any web page where substantial personal information is collected from the public. The privacy policy must state what information is being collected, why it is being collected, and how the agency will use the information. Privacy policies must be clearly labeled and easily accessed when an individual visits a web site.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.
21	<p><b>Is a privacy policy statement posted on the web site?</b></p> <p><b>Remediation Guidance:</b> If no, then <i>OMB M-99-18</i> is invoked. Agencies must post privacy policies on their principal web sites, any known major entry points, as well as any web pages where substantial personal information is collected from the public. The privacy policy must state what information is being collected, why it is being collected, and how the agency will use the information. Privacy policies must be clearly labeled and easily accessed when an individual visits a web site.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.
22	<p><b>Are web links posted anywhere on the web site?</b></p> <p><b>Remediation Guidance:</b> If no, then <i>OMB M-99-18</i> is invoked. Agencies must post privacy policies on their principal web sites, any known major entry points, as well as any web pages where substantial personal information is collected from the public. The privacy policy must state what information is being collected, why it is being collected, and how the agency will use the information. Privacy policies must be clearly labeled and easily accessed when an individual visits a web site.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
23	<p><b>Are cookies present on the web site?</b></p> <p>Note: If yes, identify types of cookies in the Comments column.</p> <p><b>Remediation Guidance:</b> If yes, persistent cookies are prohibited. Alternatively, session cookies are allowed as long as use of session cookies are indicated in the privacy policy statement, and the agency is able to demonstrate a valid need for use of these session cookies. Cookies will not knowingly be transferred to third parties unless explained in the Privacy and Security Statement.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.
24	<p><b>Does the web site have any information or pages directed at children?</b></p> <p><b>Remediation Guidance:</b> If yes, then the <i>Children's Online Privacy Protection Act (COPPA)</i>, <i>OMB M-00-13</i>, and <i>DLMS 9 Chapter 1500</i> are all invoked. Agency systems hosting web sites are mandated by OMB to comply with COPPA. This law places restrictions on the collection and use of information on any web site or online service directed to children and requires parental consent before any such collection and provides the parent with the right to see what is collected about his/her child and to restrict dissemination or use or further collection of any information about the child.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
25	<p><b>Does the web site collect PII from individuals?</b></p> <p>Note: If yes, identify what PII the system collects in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If yes, and data elements relating to United States citizens or Lawful Permanent Residents are checked under both the Identifier and Personal Information categories, then the <i>Privacy Act of 1974</i> is invoked. Agencies must meet all requirements of the Privacy Act listed under <i>5 U.S.C. 552a.(4)</i> as amended listed under "Records Maintained On Individuals."</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then the <i>HIPAA Privacy Rule, 67 FR 14775</i> may be invoked. Agencies should review this rule to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then the <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
26	<p><b>Does the web site <i>share</i> PII with internal or external parties of the Department?</b></p> <p>Note: If yes, specify with whom and for what purposes, and identify the data elements in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If yes and the information relates to United States citizens or Lawful Permanent Residents, then section (e) (6) of the Privacy Act is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, agencies must make reasonable efforts to ensure that such records are accurate, complete, timely, and relevant on each system for agency purposes. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the Act.</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then <i>HIPAA Privacy Rule, 67 FR 14775</i> may be invoked. Agencies should review these rules to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then <i>Gramm-Leach-Bliley Act (GLBA) of 1999 Pub. Law No. 106-102, 113 Stat. 1338 (1999)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.
27	<p><b>Are rules of conduct in place for access to PII on the website?</b></p> <p>Note: If yes, identify in the Comments column all categories of users with access to PII on the system, and for what purposes the PII is used.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Administrative Controls</b>					
<p><b>Note:</b> This PIA Guide uses the terms “Administrative,” “Technical,” and “Physical” to refer to security control questions—terms that are used in several federal privacy laws when referencing security requirements. USCIS recognizes the slight difference in terminology used in this guide from those that are used in other documents such as the <i>National Institute of Standards and Technology (NIST) SP 800-26, Security Self-Assessment Guide for Information Technology Systems</i>.</p>					
28	<p><b>Has the system been authorized to process information?</b></p> <p><b>Remediation Guidance:</b> If no, then the system may be required as directed by <i>OMB Circular A-130</i> to complete an accreditation for each system. Agencies should engage in an assessment process that ensures technical security features are built into the life cycle of a system.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
29	<p><b>Have there been major changes (as defined in Appendix A, “Glossary of Terms” of the PIA Questionnaire) to the system since it was last certified and accredited?</b></p> <p><b>Remediation Guidance:</b> If yes, then agencies are required by <i>OMB Circular A-130</i> to complete an update of the certification and accreditation for each system that has been modified. Agencies should engage in an assessment process that ensures existing technical security features are appropriate to the modified system.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
30	<p><b>Are security controls routinely reviewed?</b></p> <p><b>Remediation Guidance:</b> Security controls need to be routinely reviewed to ensure sustained effectiveness even when no changes to the system have occurred. <i>OMB Circular A-130</i> stipulates a system’s security controls should be reviewed “when significant modifications are made to a system, but at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system.”</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

No	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Administrative Controls</b>					
31	<p><b>Is there a system security plan for this system?</b></p> <p><b>Remediation Guidance:</b> The <i>Privacy Act of 1974</i> and <i>OMB Circular A-130</i> require procedures be in place for implementing administrative, technical, and physical security controls for systems containing a system of records. Agencies should develop a plan that demonstrates security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from NIST security guidance.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
32	<p><b>Is there a contingency (or backup) plan for the system?</b></p> <p><b>Remediation Guidance:</b> The <i>Privacy Act of 1974</i> and <i>OMB Circular A-130</i> require procedures be in place for implementing a contingency plan for systems containing a system of records. Agencies should develop a plan that demonstrates contingency security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from NIST security guidance.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
33	<p><b>Are files backed up regularly?</b></p> <p><b>Remediation Guidance:</b> <i>OMB Circular A-130</i> requires procedures be in place for protecting data on systems in the event the system and the information it contains is attacked or rendered unavailable. Agencies should devise a method for backing up information contained on the system at regular intervals.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Daily backups are performed.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Administrative Controls</b>					
34	<p><b>Are the backup files stored offsite?</b></p> <p><b>Remediation Guidance:</b>  <i>OMB Circular A-130</i> requires procedures be in place for protecting data on systems in the event the system and the information it contains is attacked or rendered unavailable. Agencies should identify an alternative site for housing backup files.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	DOJ is responsible for the backups.
35	<p><b>Are there user manuals for the system?</b></p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
36	<p><b>Have personnel using the system been trained and made aware of their responsibilities for protecting personal information being collected and maintained?</b></p> <p><b>Remediation Guidance:</b>                      If no, <i>OMB Circular A-130</i> requires that each agency ensure the security of information contained on each system to include training of users and employees of security controls in place. Agencies should provide users with training of their roles and responsibilities for protecting PII collected and maintained on the system.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
37	<p><b>Who will have access to the PII on the system?</b></p> <p>Note: Check all that apply in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Users <input checked="" type="checkbox"/> Administrators <input checked="" type="checkbox"/> Developers <input checked="" type="checkbox"/> Contractors
38	<p><b>Are methods in place to ensure least privilege (e.g., "need to know" and accountability)?</b></p> <p>Note: If yes, please specify method(s) in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Technical Controls</b>					
39	<p><b>Are technical controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system?</b></p> <p>Note: If yes, check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, <i>OMB Circular A-130</i> requires that each agency ensure the security of information contained on each system by implementing technical security controls. Agencies should devise administrative, technical, and physical controls for each system to protect the PII it contains.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>USCIS has established technical control requirements including the following controls:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> User ID</li> <li><input checked="" type="checkbox"/> Passwords</li> <li><input checked="" type="checkbox"/> Firewall</li> <li><input type="checkbox"/> Virtual Private Network (VPN)</li> <li><input type="checkbox"/> Encryption</li> <li><input type="checkbox"/> Intrusion Detection System (IDS)</li> <li><input type="checkbox"/> Common Access Cards (CAC)</li> <li><input type="checkbox"/> Smart Cards</li> <li><input type="checkbox"/> Biometrics</li> <li><input type="checkbox"/> Public Key Infrastructure (PKI)</li> </ul>
40	<p><b>Are the following password controls in place?</b></p> <p>Note: Check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, <i>OMB Circular A-130</i> requires that each agency ensure the security of information contained on each system. Agencies should implement one or more of the password controls for each system to protect the PII it contains.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Passwords expire after a set period of time.</li> <li><input checked="" type="checkbox"/> Accounts are locked after a set period of inactivity.</li> <li><input checked="" type="checkbox"/> Minimum length of passwords is eight characters.</li> <li><input checked="" type="checkbox"/> Passwords must be a combination of uppercase, lowercase, and special characters.</li> <li><input checked="" type="checkbox"/> Accounts are locked after a set number of incorrect attempts.</li> </ul> <p>USCIS has established password management security requirements</p>
41	<p><b>Is a process in place to monitor and respond to incidents?</b></p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Physical Controls</b>					
42	<p><b>Are physical access controls in place?</b></p> <p>Note: If yes, check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, <i>OMB Circular A-130</i> requires that each agency ensure the security of information contained on each system by implementing technical security controls. Agencies should devise administrative, technical, and physical controls for each system to protect the PII it contains.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>USCIS controls include:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Guards</li> <li><input checked="" type="checkbox"/> Identification Badges</li> <li><input checked="" type="checkbox"/> Key Cards</li> <li><input type="checkbox"/> Cipher Locks</li> <li><input type="checkbox"/> Biometrics</li> <li><input type="checkbox"/> Closed Circuit TV (CCTV)</li> <li><input type="checkbox"/> Other _____</li> <li><input type="checkbox"/> Other _____</li> <li><input type="checkbox"/> Other _____</li> </ul>

### APPENDIX D – PIA QUESTIONNAIRE -- RNACS

**NOTE:** Based on current privacy regulation and guidance, the PIA should be performed on the production environment. For those systems that have test and development environments, those environments may or may not warrant their own Privacy Impact Assessment (PIA). The test and development environments generally do not necessitate a separate PIA, however, the assessor may need to consult information technology (IT) system policy guides and/or his or her security officer and/or the Office of the Chief Information Officer (OCIO) for firm technical decisions. For those systems that have performed risk assessments and defined system boundaries and scope, the system characterization will likely be the same for both that risk assessment and this PIA. PIAs performed at the initiation of the system development life cycle will require conducting another PIA at intervals stipulated by the security handbook when significant changes occur to the system.

The PIA attempts to determine what kind of personal information is contained within a system, what is done with that information, and how that information is protected. There are many requirements for systems containing personal information based on an extensive list of privacy regulations and guidance. The information guidance provides a checklist of requirements for meeting certain requirements. However, users should consult the privacy law decisions have updated legal provisions of the Privacy Act from the Privacy Officer can answer questions related to the specific details of privacy law. The OCIO can answer questions related to the administrative, technical, and physical controls on the system and related systems. A full list of questionnaire questions.

**System Name:** United States Citizenship and Immigration Services (USCIS)  
Reengineered Naturalization Casework System (RNACS)

**System Environment (production, test, development, or other. If other, please explain):** Production

**System Location (entity/contractor name of site, building, room, city, and state):** Department of Justice Data Center, Dallas, TX

**Activity/Purpose of System:** To track, process and report on applications for immigration benefits (naturalization and citizenship).

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>System Characterization</b>					
1	<p><b>Does USCIS own the system?</b></p> <p>Note: If no, identify the system owner in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Owner: (b)(7)
2	<p><b>Does USCIS operate the system?</b></p> <p>Note: If no, identify the system operator in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3	<p><b>Identify in the Comments column the life-cycle phase of this system.</b></p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Initiation <input type="checkbox"/> Develop/Acquisition <input type="checkbox"/> Implementation <input checked="" type="checkbox"/> Operations/Maintenance <input type="checkbox"/> Disposal
4	<p><b>Is the system a stand-alone system (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire)?</b></p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5	<p><b>Is the system network-connected (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire)?</b></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	<p><b>Is the system a General Support System (GSS), Major Application (MA) or sensitive system (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire)?</b></p> <p>Note: If yes, identify whether the system is a GSS, MA or sensitive system in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Sensitive But Unclassified

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>System Characterization</b>					
7	<p><b>Does the system contain PII within any database(s), record(s), file(s) or document(s)?</b></p> <p>Note: If yes, check all that apply in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If the system contains no records with any data elements listed in the comments section, the system is not subject to federal privacy laws or regulations such as the <i>Privacy Act of 1974</i>. Questions 8-18 may be marked with an "N/A."</p> <p>If data elements relating to persons who are either United States Citizens or Lawful Permanent Residents are checked under the personal information category in the comments column, then the <i>Privacy Act of 1974</i> is invoked. Agencies must meet all requirements of the Privacy Act listed under 5 U.S.C. 552a.(4) as amended, listed under "Records Maintained On Individuals."</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then the <i>HIPAA Privacy Rule 67 FR 14775</i> may be invoked. Agencies should review this rule to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then the <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p><b>Personal Information:</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Name</li> <li><input checked="" type="checkbox"/> Date of Birth</li> <li><input checked="" type="checkbox"/> Social Security Number (or other number originated by a government that specifically identifies an individual)</li> <li><input type="checkbox"/> Photographic Identifiers (e.g., photograph image, x-rays, and video)</li> <li><input type="checkbox"/> Driver's License</li> <li><input type="checkbox"/> Biometric Identifiers (e.g., fingerprint and voiceprint)</li> <li><input type="checkbox"/> Mother's Maiden Name</li> <li><input type="checkbox"/> Vehicle Identifiers (e.g., license plates)</li> <li><input checked="" type="checkbox"/> Mailing Address</li> <li><input type="checkbox"/> Phone Numbers (e.g., phone, fax, and cell)</li> <li><input type="checkbox"/> Medical Records Numbers</li> <li><input type="checkbox"/> Medical Notes</li> <li><input type="checkbox"/> Financial Account Information and/or Numbers (e.g., checking account number and PINs)</li> <li><input type="checkbox"/> Certificates (e.g., birth, death, and marriage)</li> <li><input type="checkbox"/> Legal Documents or Notes (e.g., divorce decree, criminal records, or other)</li> <li><input type="checkbox"/> Device Identifiers (e.g., pacemaker, hearing aid, or other)</li> <li><input type="checkbox"/> Web URLs</li> <li><input type="checkbox"/> Email Address</li> <li><input type="checkbox"/> Education Records</li> <li><input checked="" type="checkbox"/> Other: Alien Number (A-Number)</li> </ul>

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>System Characterization</b>					
8	<p><b>Has a Privacy Act Systems of Records Notice (PARN) been published in the Federal Register?</b></p> <p><b>Remediation Guidance:</b> If no, and the system meets the definition of a System of Records, then the <i>Privacy Act of 1974</i> requirements are invoked. Agencies must develop a PARN and publish the notice in the Federal Register with appropriate specifications listed in <i>5 U.S.C. Section 552a</i> as amended.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>Federal Register Notice published 04/29/02</p> <p>67FR20996</p>
9	<p><b>Have major changes (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire) to the system been made since publication of the PARN?</b></p> <p><b>Remediation Guidance:</b> If yes, then the <i>Privacy Act of 1974</i> requires that agencies publish in the Federal Register a notice of any, and all revisions to the existence and character of the system of records with appropriate specifications listed in <i>5 U.S.C. Section 552a</i> as amended.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	<p><b>Does the PARN address all required categories of information?</b></p> <p>Note: Check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, then the notice specifying the existence of the system of records will include all criteria listed in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> System Name</li> <li><input type="checkbox"/> Security Classification</li> <li><input checked="" type="checkbox"/> System Location</li> <li><input checked="" type="checkbox"/> Categories of Individuals Covered by the System</li> <li><input checked="" type="checkbox"/> Categories of Records in the System</li> <li><input checked="" type="checkbox"/> Authority of Maintenance of the System</li> <li><input checked="" type="checkbox"/> Purpose</li> <li><input checked="" type="checkbox"/> Routine Uses of Records Maintained in the System</li> <li><input type="checkbox"/> Disclosure to Consumer Reporting Agencies</li> <li><input checked="" type="checkbox"/> Policies and Practices for Storing, Retrieving, Accessing, Retaining and Disposing of Records</li> <li><input checked="" type="checkbox"/> System Manager(s) and Address</li> <li><input checked="" type="checkbox"/> Notification Procedure</li> <li><input checked="" type="checkbox"/> Record Access Procedure</li> <li><input checked="" type="checkbox"/> Contesting Record Procedure</li> <li><input checked="" type="checkbox"/> Record Source Categories</li> <li><input checked="" type="checkbox"/> Systems Exempted From Certain Provisions of the Act</li> </ul>

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
11	<p><b>Does the system collect PII from individuals?</b></p> <p>Note: If yes, identify the PII the system collects directly from individuals in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> Each agency maintaining system of records is required to collect information to the greatest extent practicable directly from the individual when information may result in adverse determinations about an individual's rights, benefits, and privileges under federal programs.</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then <i>HIPAA Privacy Rule 67 FR 14775</i> may be invoked. Agencies should review these rules to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p><b>Personal Information:</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Alien Registration Number</li> <li><input checked="" type="checkbox"/> Name</li> <li><input checked="" type="checkbox"/> Date of Birth</li> <li><input type="checkbox"/> Social Security Number (or other number originated by a government that specifically identifies an individual)</li> <li><input type="checkbox"/> Photographic Identifiers (e.g., photograph image, x-rays, and video)</li> <li><input type="checkbox"/> Driver's License</li> <li><input type="checkbox"/> Biometric Identifiers (e.g., fingerprint and voiceprint)</li> <li><input type="checkbox"/> Mother's Maiden Name</li> <li><input type="checkbox"/> Vehicle Identifiers (e.g., license plates)</li> <li><input checked="" type="checkbox"/> Mailing Address</li> <li><input type="checkbox"/> Phone Numbers (e.g., phone, fax, and cell)</li> <li><input type="checkbox"/> Medical Records Numbers</li> <li><input type="checkbox"/> Medical Notes</li> <li><input type="checkbox"/> Financial Account Information and/or Numbers (e.g., checking account number and PINs)</li> <li><input type="checkbox"/> Certificates (e.g., birth, death, and marriage)</li> <li><input type="checkbox"/> Legal Documents or Notes (e.g., divorce decree, criminal records, or other)</li> <li><input type="checkbox"/> Device Identifiers (e.g., pacemaker, hearing aid, or other)</li> <li><input type="checkbox"/> Web URLs</li> <li><input type="checkbox"/> E-mail Address</li> <li><input type="checkbox"/> Education Records</li> <li><input type="checkbox"/> Other: _____</li> </ul>

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
12	<p><b>Does the system collect PII from other sources (e.g., databases, websites, etc.)?</b></p> <p>Note: If yes, specify the source(s) and PII collected in the Comments column.</p> <p><b>Remediation Guidance:</b> If yes, then each agency is required to maintain records on systems that are used for making determinations about an individual with accuracy, relevance, timeliness, and completeness as reasonably necessary to assure fairness to the individual. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the <i>Privacy Act of 1974</i>.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Name Check Response (IBIS, FBI) Fingerprint Response (FBI) Cases, Status Updates (C4)
13	<p><b>Does the system populate data for other resources (i.e., do databases, web sites, or other resources rely on this system's data)?</b></p> <p>Note: If yes, specify resource(s) and purpose for each instance in the Comments column.</p> <p><b>Remediation Guidance:</b> If yes, then section (e) (6) of the <i>Privacy Act of 1974</i> is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, the agency must make reasonable efforts to assure that such records are accurate, complete, timely, and relevant on each system for agency purposes. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the Act.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Transfer of cases to C4

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
14	<p><b>Does the system <i>share</i> PII with internal or external parties of USCIS?</b></p> <p>Note: If yes, identify in the Comments column which data elements are shared. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If yes, then section (e) (6) of the <i>Privacy Act of 1974</i> is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, agencies must make reasonable efforts to ensure that such records are accurate, complete, timely, and relevant on each system for agency purposes. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the Act.</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then <i>HIPAA Privacy Rule, 67 FR 14775</i> may be invoked. Agencies should review these rules to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Update of Central Index with naturalization data

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
15	<p><b>Are records on the system retrievable?</b></p> <p>Note: If yes, specify in the Comments column what method is used in retrieving the records (i.e., using a record number, name, social security number, or other data element or record locator methodology). If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If yes, then a system of records in which information relating to a United States citizen or Lawful Permanent Resident is retrieved using one or more of an individual's "identifying information" invokes <i>Privacy Act of 1974</i> requirements. All requirements under <i>5 U.S.C. of Section 552a</i> as amended must be met by an agency for this system.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	On-line queries Reports
16	<p><b>Is there a notification process in place when changes occur (i.e., revisions to PII or when the system encounters a major change or is replaced) for alerting other resources dependent upon PII contained on this system?</b></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
17	<p><b>Are processes in place for periodic review of PII contained in the system to ensure it is timely, accurate, and relevant?</b></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
18	<p><b>Are rules of conduct in place for access to PII on the system?</b></p> <p>Note: If yes, identify in the Comments column all users with access to PII on the system, and for what purposes they use the PII.</p> <p><b>Remediation Guidance:</b> If no, then Section (e)(9-10) of the <i>Privacy Act of 1974</i> is invoked to the extent that the system contains information relating to United States citizens or Lawful Permanent Residents. The Act requires rules of conduct for persons involved in the design, development, operations, or maintenance of a system's PII.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p><input checked="" type="checkbox"/> Users  <input checked="" type="checkbox"/> Administrators  <input checked="" type="checkbox"/> Developers  <input checked="" type="checkbox"/> Contractors</p> <p>For what purposes:  <input type="checkbox"/> _____  <input type="checkbox"/> _____  <input type="checkbox"/> _____  <input type="checkbox"/> _____</p> <p>All users listed will be subject to USCIS and Rules of Behavior</p>
19	<p><b>Does the system host a web site either as an Internet, an intranet, or both?</b></p> <p>Note: If yes, identify what type of site in the Comments column.</p> <p>Note: If no, check N/A for all subsequent questions in the "Web Site Host Question Sets" section and answer questions starting with the "Administrative Controls" section beginning with Question #28.</p> <p><b>Remediation Guidance:</b> If yes, then <i>OMB M-99-18</i> is invoked requiring that for every federal, public web site agencies include a privacy policy statement, even if the site does <i>not</i> collect any information and does not create a Privacy Act record.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
20	<p><b>Is the web site accessible by the public or other entities (i.e., contractors, third party administrators, state, or local agencies, etc.)?</b></p> <p><b>Remediation Guidance:</b> If yes, then <i>OMB M-99-18</i> is invoked. Agencies must post privacy policies on their principal web sites, any known major entry points, and any web page where substantial personal information is collected from the public. The privacy policy must state what information is being collected, why it is being collected, and how the agency will use the information. Privacy policies must be clearly labeled and easily accessed when an individual visits a web site.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.
21	<p><b>Is a privacy policy statement posted on the web site?</b></p> <p><b>Remediation Guidance:</b> If no, then <i>OMB M-99-18</i> is invoked. Agencies must post privacy policies on their principal web sites, any known major entry points, as well as any web pages where substantial personal information is collected from the public. The privacy policy must state what information is being collected, why it is being collected, and how the agency will use the information. Privacy policies must be clearly labeled and easily accessed when an individual visits a web site.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.
22	<p><b>Are web links posted anywhere on the web site?</b></p> <p><b>Remediation Guidance:</b> If no, then <i>OMB M-99-18</i> is invoked. Agencies must post privacy policies on their principal web sites, any known major entry points, as well as any web pages where substantial personal information is collected from the public. The privacy policy must state what information is being collected, why it is being collected, and how the agency will use the information. Privacy policies must be clearly labeled and easily accessed when an individual visits a web site.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
23	<p><b>Are cookies present on the web site?</b></p> <p>Note: If yes, identify types of cookies in the Comments column.</p> <p><b>Remediation Guidance:</b> If yes, persistent cookies are prohibited. Alternatively, session cookies are allowed as long as use of session cookies are indicated in the privacy policy statement, and the agency is able to demonstrate a valid need for use of these session cookies. Cookies will not knowingly be transferred to third parties unless explained in the Privacy and Security Statement.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.
24	<p><b>Does the web site have any information or pages directed at children?</b></p> <p><b>Remediation Guidance:</b> If yes, then the <i>Children's Online Privacy Protection Act (COPPA)</i>, <i>OMB M-00-13</i>, and <i>DLMS 9 Chapter 1500</i> are all invoked. Agency systems hosting web sites are mandated by OMB to comply with COPPA. This law places restrictions on the collection and use of information on any web site or online service directed to children and requires parental consent before any such collection and provides the parent with the right to see what is collected about his/her child and to restrict dissemination or use or further collection of any information about the child.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
25	<p><b>Does the web site collect PII from individuals?</b></p> <p>Note: If yes, identify what PII the system collects in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If yes, and data elements relating to United States citizens or Lawful Permanent Residents are checked under both the Identifier and Personal Information categories, then the <i>Privacy Act of 1974</i> is invoked. Agencies must meet all requirements of the Privacy Act listed under <i>5 U.S.C. 552a.(4)</i> as amended listed under "Records Maintained On Individuals."</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then the <i>HIPAA Privacy Rule, 67 FR 14775</i> may be invoked. Agencies should review this rule to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then the <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
26	<p><b>Does the web site <i>share</i> PII with internal or external parties of the Department?</b></p> <p>Note: If yes, specify with whom and for what purposes, and identify the data elements in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If yes and the information relates to United States citizens or Lawful Permanent Residents, then section (e) (6) of the Privacy Act is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, agencies must make reasonable efforts to ensure that such records are accurate, complete, timely, and relevant on each system for agency purposes. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the Act.</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then <i>HIPAA Privacy Rule, 67 FR 14775</i> may be invoked. Agencies should review these rules to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then <i>Gramm-Leach-Bliley Act (GLBA) of 1999 Pub. Law No. 106-102, 113 Stat. 1338 (1999)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.
27	<p><b>Are rules of conduct in place for access to PII on the website?</b></p> <p>Note: If yes, identify in the Comments column all categories of users with access to PII on the system, and for what purposes the PII is used.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Administrative Controls</b>					
<p><b>Note:</b> This PIA Guide uses the terms "Administrative," "Technical," and "Physical" to refer to security control questions—terms that are used in several federal privacy laws when referencing security requirements. USCIS recognizes the slight difference in terminology used in this guide from those that are used in other documents such as the <i>National Institute of Standards and Technology (NIST) SP 800-26, Security Self-Assessment Guide for Information Technology Systems</i>.</p>					
28	<p><b>Has the system been authorized to process information?</b></p> <p><b>Remediation Guidance:</b> If no, then the system may be required as directed by <i>OMB Circular A-130</i> to complete an accreditation for each system. Agencies should engage in an assessment process that ensures technical security features are built into the life cycle of a system.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
29	<p><b>Have there been major changes (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire) to the system since it was last certified and accredited?</b></p> <p><b>Remediation Guidance:</b> If yes, then agencies are required by <i>OMB Circular A-130</i> to complete an update of the certification and accreditation for each system that has been modified. Agencies should engage in an assessment process that ensures existing technical security features are appropriate to the modified system.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
30	<p><b>Are security controls routinely reviewed?</b></p> <p><b>Remediation Guidance:</b> Security controls need to be routinely reviewed to ensure sustained effectiveness even when no changes to the system have occurred. <i>OMB Circular A-130</i> stipulates a system's security controls should be reviewed "when significant modifications are made to a system, but at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system."</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Administrative Controls</b>					
31	<p><b>Is there a system security plan for this system?</b></p> <p><b>Remediation Guidance:</b>                      The <i>Privacy Act of 1974</i> and <i>OMB Circular A-130</i> require procedures be in place for implementing administrative, technical, and physical security controls for systems containing a system of records. Agencies should develop a plan that demonstrates security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from NIST security guidance.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Sensitive System Security Plan, Jan 04
32	<p><b>Is there a contingency (or backup) plan for the system?</b></p> <p><b>Remediation Guidance:</b>                      The <i>Privacy Act of 1974</i> and <i>OMB Circular A-130</i> require procedures be in place for implementing a contingency plan for systems containing a system of records. Agencies should develop a plan that demonstrates contingency security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from NIST security guidance.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Y2K Contingency Plan Backup procedures controlled by IDMS and DOJ Security software ("TOP SECRET")
33	<p><b>Are files backed up regularly?</b></p> <p><b>Remediation Guidance:</b>  <i>OMB Circular A-130</i> requires procedures be in place for protecting data on systems in the event the system and the information it contains is attacked or rendered unavailable. Agencies should devise a method for backing up information contained on the system at regular intervals.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Administrative Controls</b>					
34	<p><b>Are the backup files stored offsite?</b></p> <p><b>Remediation Guidance:</b> OMB Circular A-130 requires procedures be in place for protecting data on systems in the event the system and the information it contains is attacked or rendered unavailable. Agencies should identify an alternative site for housing backup files.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
35	<p><b>Are there user manuals for the system?</b></p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
36	<p><b>Have personnel using the system been trained and made aware of their responsibilities for protecting personal information being collected and maintained?</b></p> <p><b>Remediation Guidance:</b> If no, OMB Circular A-130 requires that each agency ensure the security of information contained on each system to include training of users and employees of security controls in place. Agencies should provide users with training of their roles and responsibilities for protecting PII collected and maintained on the system.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
37	<p><b>Who will have access to the PII on the system?</b></p> <p>Note: Check all that apply in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Users <input checked="" type="checkbox"/> Administrators <input checked="" type="checkbox"/> Developers <input checked="" type="checkbox"/> Contractors
38	<p><b>Are methods in place to ensure least privilege (e.g., "need to know" and accountability)?</b></p> <p>Note: If yes, please specify method(s) in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Levels of access are conferred by (1) PICS and (2) supervisory staff at local office

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Technical Controls</b>					
39	<p><b>Are technical controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system?</b></p> <p>Note: If yes, check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, <i>OMB Circular A-130</i> requires that each agency ensure the security of information contained on each system by implementing technical security controls. Agencies should devise administrative, technical, and physical controls for each system to protect the PII it contains.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>USCIS has established technical control requirements including the following controls:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> User ID</li> <li><input checked="" type="checkbox"/> Passwords</li> <li><input checked="" type="checkbox"/> Firewall</li> <li><input type="checkbox"/> Virtual Private Network (VPN)</li> <li><input type="checkbox"/> Encryption</li> <li><input type="checkbox"/> Intrusion Detection System (IDS)</li> <li><input type="checkbox"/> Common Access Cards (CAC)</li> <li><input type="checkbox"/> Smart Cards</li> <li><input type="checkbox"/> Biometrics</li> <li><input type="checkbox"/> Public Key Infrastructure (PKI)</li> </ul>
40	<p><b>Are the following password controls in place?</b></p> <p>Note: Check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, <i>OMB Circular A-130</i> requires that each agency ensure the security of information contained on each system. Agencies should implement one or more of the password controls for each system to protect the PII it contains.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Passwords expire after a set period of time.</li> <li><input type="checkbox"/> Accounts are locked after a set period of inactivity.</li> <li><input checked="" type="checkbox"/> Minimum length of passwords is eight characters.</li> <li><input checked="" type="checkbox"/> Passwords must be a combination of uppercase, lowercase, and special characters.</li> <li><input checked="" type="checkbox"/> Accounts are locked after a set number of incorrect attempts.</li> </ul> <p>USCIS has established password management security requirements</p>
41	<p><b>Is a process in place to monitor and respond to incidents?</b></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Physical Controls</b>					
42	<p><b>Are physical access controls in place?</b></p> <p>Note: If yes, check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, <i>OMB Circular A-130</i> requires that each agency ensure the security of information contained on each system by implementing technical security controls. Agencies should devise administrative, technical, and physical controls for each system to protect the PII it contains.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>USCIS controls include:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Guards</li> <li><input checked="" type="checkbox"/> Identification Badges</li> <li><input checked="" type="checkbox"/> Key Cards</li> <li><input type="checkbox"/> Cipher Locks</li> <li><input type="checkbox"/> Biometrics</li> <li><input checked="" type="checkbox"/> Closed Circuit TV (CCTV)</li> <li><input type="checkbox"/> Other _____</li> <li><input type="checkbox"/> Other _____</li> <li><input type="checkbox"/> Other _____</li> </ul>

**APPENDIX D – PIA QUESTIONNAIRE -- RAPS**

**NOTE:** Based on current privacy regulation and guidance, the PIA should be performed on the production environment. For those systems that have test and development environments, those environments may or may not warrant their own Privacy Impact Assessment (PIA). If test and development environments generally do not necessitate a separate PIA, however, the assessor may need to consult internal technology (IT) system policy guidance and/or his or her security officer and/or the Office of the Chief Information Officer (OCIO) to confirm such decisions. For those systems that have performed risk assessments and defined system boundaries and scopes, the system characterization will likely be necessary on both the risk assessment and this PIA. PIAs should be performed immediately after the system development is complete, while the system is producing and on a regular interval as stipulated by the Security Handbook when significant changes occur to the system.

The PIA attempts to determine what kind of personal information is contained within a system, what is done with that information, and how that information is protected. There are many requirements for system storage of personal information, based on an extensive state and federal regulations, and guidance for information guidance provided gives users a starting point for their decision environment. However, users should be informed that privacy assessment decisions have updated the content provisions of the Privacy Act statute. The Privacy Officer can answer questions related to the technicalities of privacy law. The OCIO can answer questions related to the high level, technical, and physical controls of the system, and includes as well as a list of privacy questions.

**System Name:** United States Citizenship and Immigration Services (USCIS)  
Refugees, Asylum, and Parole System (RAPS)

**System Environment** (production, test, development, or other. If other, please explain): Production

**System Location** (entity/contractor name of site, building, room, city, and state): DOJ Data Center, Dallas, TX

**Activity/Purpose of System:** To track, process and report on applications for immigration benefits (Asylum).

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>System Characterization</b>					
1	Does USCIS own the system?  Note: If no, identify the system owner in the Comments column.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Owner: <b>b(6)</b>
2	Does USCIS operate the system?  Note: If no, identify the system operator in the Comments column.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3	Identify in the Comments column the life-cycle phase of this system.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Initiation <input type="checkbox"/> Develop/Acquisition <input type="checkbox"/> Implementation <input checked="" type="checkbox"/> Operations/Maintenance <input type="checkbox"/> Disposal
4	Is the system a stand-alone system (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire)?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5	Is the system network-connected (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire)?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Is the system a General Support System (GSS), Major Application (MA) or sensitive system (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire)?  Note: If yes, identify whether the system is a GSS, MA or sensitive system in the Comments column.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Sensitive But Unclassified

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>System Characterization</b>					
7	<p><b>Does the system contain PII within any database(s), record(s), file(s) or document(s)?</b></p> <p>Note: If yes, check all that apply in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If the system contains no records with any data elements listed in the comments section, the system is not subject to federal privacy laws or regulations such as the <i>Privacy Act of 1974</i>. Questions 8-18 may be marked with an "N/A."</p> <p>If data elements relating to persons who are either United States Citizens or Lawful Permanent Residents are checked under the personal information category in the comments column, then the <i>Privacy Act of 1974</i> is invoked. Agencies must meet all requirements of the Privacy Act listed under 5 U.S.C. 552a.(4) as amended, listed under "Records Maintained On Individuals."</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then the <i>HIPAA Privacy Rule 67 FR 14775</i> may be invoked. Agencies should review this rule to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then the <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p><b>Personal Information:</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Name</li> <li><input checked="" type="checkbox"/> Date of Birth</li> <li><input checked="" type="checkbox"/> Social Security Number (or other number originated by a government that specifically identifies an individual)</li> <li><input type="checkbox"/> Photographic Identifiers (e.g., photograph image, x-rays, and video)</li> <li><input type="checkbox"/> Driver's License</li> <li><input type="checkbox"/> Biometric Identifiers (e.g., fingerprint and voiceprint)</li> <li><input type="checkbox"/> Mother's Maiden Name</li> <li><input type="checkbox"/> Vehicle Identifiers (e.g., license plates)</li> <li><input checked="" type="checkbox"/> Mailing Address</li> <li><input type="checkbox"/> Phone Numbers (e.g., phone, fax, and cell)</li> <li><input type="checkbox"/> Medical Records Numbers</li> <li><input type="checkbox"/> Medical Notes</li> <li><input type="checkbox"/> Financial Account Information and/or Numbers (e.g., checking account number and PINs)</li> <li><input type="checkbox"/> Certificates (e.g., birth, death, and marriage)</li> <li><input type="checkbox"/> Legal Documents or Notes (e.g., divorce decree, criminal records, or other)</li> <li><input type="checkbox"/> Device Identifiers (e.g., pacemaker, hearing aid, or other)</li> <li><input type="checkbox"/> Web URLs</li> <li><input type="checkbox"/> Email Address</li> <li><input type="checkbox"/> Education Records</li> <li><input checked="" type="checkbox"/> Other: Alien Number (A-Number)</li> </ul>

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>System Characterization</b>					
8	<p><b>Has a Privacy Act Systems of Records Notice (PARN) been published in the Federal Register?</b></p> <p><b>Remediation Guidance:</b> If no, and the system meets the definition of a System of Records, then the <i>Privacy Act of 1974</i> requirements are invoked. Agencies must develop a PARN and publish the notice in the Federal Register with appropriate specifications listed in <i>5 U.S.C. Section 552a</i> as amended.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Federal Register notice is currently with General Counsel for review before publication
9	<p><b>Have major changes (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire) to the system been made since publication of the PARN?</b></p> <p><b>Remediation Guidance:</b> If yes, then the <i>Privacy Act of 1974</i> requires that agencies publish in the Federal Register a notice of any, and all revisions to the existence and character of the system of records with appropriate specifications listed in <i>5 U.S.C. Section 552a</i> as amended.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
10	<p><b>Does the PARN address all required categories of information?</b></p> <p>Note: Check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, then the notice specifying the existence of the system of records will include all criteria listed in the Comments column.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> System Name <input type="checkbox"/> Security Classification <input checked="" type="checkbox"/> System Location <input checked="" type="checkbox"/> Categories of Individuals Covered by the System <input checked="" type="checkbox"/> Categories of Records in the System <input checked="" type="checkbox"/> Authority of Maintenance of the System <input checked="" type="checkbox"/> Purpose <input checked="" type="checkbox"/> Routine Uses of Records Maintained in the System <input type="checkbox"/> Disclosure to Consumer Reporting Agencies <input checked="" type="checkbox"/> Policies and Practices for Storing, Retrieving, Accessing, Retaining and Disposing of Records <input checked="" type="checkbox"/> System Manager(s) and Address <input checked="" type="checkbox"/> Notification Procedure <input checked="" type="checkbox"/> Record Access Procedure <input checked="" type="checkbox"/> Contesting Record Procedure <input checked="" type="checkbox"/> Record Source Categories <input checked="" type="checkbox"/> Systems Exempted From Certain Provisions of the Act

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
11	<p><b>Does the system collect PII from individuals?</b></p> <p>Note: If yes, identify the PII the system collects directly from individuals in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> Each agency maintaining system of records is required to collect information to the greatest extent practicable directly from the individual when information may result in adverse determinations about an individual's rights, benefits, and privileges under federal programs.</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then <i>HIPAA Privacy Rule 67 FR 14775</i> may be invoked. Agencies should review these rules to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p><b>Personal Information:</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Alien Registration Number</li> <li><input checked="" type="checkbox"/> Name</li> <li><input checked="" type="checkbox"/> Date of Birth</li> <li><input checked="" type="checkbox"/> Social Security Number (or other number originated by a government that specifically identifies an individual)</li> <li><input type="checkbox"/> Photographic Identifiers (e.g., photograph image, x-rays, and video)</li> <li><input type="checkbox"/> Driver's License</li> <li><input type="checkbox"/> Biometric Identifiers (e.g., fingerprint and voiceprint)</li> <li><input type="checkbox"/> Mother's Maiden Name</li> <li><input type="checkbox"/> Vehicle Identifiers (e.g., license plates)</li> <li><input checked="" type="checkbox"/> Mailing Address</li> <li><input type="checkbox"/> Phone Numbers (e.g., phone, fax, and cell)</li> <li><input type="checkbox"/> Medical Records Numbers</li> <li><input type="checkbox"/> Medical Notes</li> <li><input type="checkbox"/> Financial Account Information and/or Numbers (e.g., checking account number and PINs)</li> <li><input type="checkbox"/> Certificates (e.g., birth, death, and marriage)</li> <li><input type="checkbox"/> Legal Documents or Notes (e.g., divorce decree, criminal records, or other)</li> <li><input type="checkbox"/> Device Identifiers (e.g., pacemaker, hearing aid, or other)</li> <li><input type="checkbox"/> Web URLs</li> <li><input type="checkbox"/> E-mail Address</li> <li><input type="checkbox"/> Education Records</li> <li><input type="checkbox"/> Other: _____</li> </ul>

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
12	<p><b>Does the system collect PII from other sources (e.g., databases, websites, etc.)?</b></p> <p>Note: If yes, specify the source(s) and PII collected in the Comments column.</p> <p><b>Remediation Guidance:</b> If yes, then each agency is required to maintain records on systems that are used for making determinations about an individual with accuracy, relevance, timeliness, and completeness as reasonably necessary to assure fairness to the individual. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the <i>Privacy Act of 1974</i>.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>Name Check Responses (IBIS, FBI) Fingerprint Responses (FBI) Presence of records in DACS, NAILS, APSS Presence of A-File (NFTS) Attorney address (PAMS) Address data (C3)</p>
13	<p><b>Does the system populate data for other resources (i.e., do databases, web sites, or other resources rely on this system's data)?</b></p> <p>Note: If yes, specify resource(s) and purpose for each instance in the Comments column.</p> <p><b>Remediation Guidance:</b> If yes, then section (e) (6) of the <i>Privacy Act of 1974</i> is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, the agency must make reasonable efforts to assure that such records are accurate, complete, timely, and relevant on each system for agency purposes. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the Act.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>Creation of new A-File (CIS) A-File receipt (CIS) Case status (CIS) Office of Refugee Resettlement (quarterly counts of asylum grants) Creation of NTAs (DACs)</p>

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
14	<p><b>Does the system <i>share</i> PII with internal or external parties of USCIS?</b></p> <p>Note: If yes, identify in the Comments column which data elements are shared. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If yes, then section (e) (6) of the <i>Privacy Act of 1974</i> is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, agencies must make reasonable efforts to ensure that such records are accurate, complete, timely, and relevant on each system for agency purposes. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the Act.</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then <i>HIPAA Privacy Rule, 67 FR 14775</i> may be invoked. Agencies should review these rules to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
15	<p><b>Are records on the system retrievable?</b></p> <p>Note: If yes, specify in the Comments column what method is used in retrieving the records (i.e., using a record number, name, social security number, or other data element or record locator methodology). If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If yes, then a system of records in which information relating to a United States citizen or Lawful Permanent Resident is retrieved using one or more of an individual's "identifying information" invokes <i>Privacy Act of 1974</i> requirements. All requirements under <i>5 U.S.C. of Section 552a</i> as amended must be met by an agency for this system.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	On-line queries Reports
16	<p><b>Is there a notification process in place when changes occur (i.e., revisions to PII or when the system encounters a major change or is replaced) for alerting other resources dependent upon PII contained on this system?</b></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
17	<p><b>Are processes in place for periodic review of PII contained in the system to ensure it is timely, accurate, and relevant?</b></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
18	<p><b>Are rules of conduct in place for access to PII on the system?</b></p> <p>Note: If yes, identify in the Comments column all users with access to PII on the system, and for what purposes they use the PII.</p> <p><b>Remediation Guidance:</b> If no, then Section (e)(9-10) of the <i>Privacy Act of 1974</i> is invoked to the extent that the system contains information relating to United States citizens or Lawful Permanent Residents. The Act requires rules of conduct for persons involved in the design, development, operations, or maintenance of a system's PII.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p><input checked="" type="checkbox"/> Users  <input checked="" type="checkbox"/> Administrators  <input checked="" type="checkbox"/> Developers  <input checked="" type="checkbox"/> Contractors</p> <p>For what purposes:  <input type="checkbox"/> _____  <input type="checkbox"/> _____  <input type="checkbox"/> _____  <input type="checkbox"/> _____</p> <p>All users listed will be subject to USCIS and Rules of Behavior</p>
19	<p><b>Does the system host a web site either as an Internet, an intranet, or both?</b></p> <p>Note: If yes, identify what type of site in the Comments column.</p> <p>Note: If no, check N/A for all subsequent questions in the "Web Site Host Question Sets" section and answer questions starting with the "Administrative Controls" section beginning with Question #28.</p> <p><b>Remediation Guidance:</b> If yes, then <i>OMB M-99-18</i> is invoked requiring that for every federal, public web site agencies include a privacy policy statement, even if the site does <i>not</i> collect any information and does not create a Privacy Act record.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
20	<p><b>Is the web site accessible by the public or other entities (i.e., contractors, third party administrators, state, or local agencies, etc.)?</b></p> <p><b>Remediation Guidance:</b> If yes, then <i>OMB M-99-18</i> is invoked. Agencies must post privacy policies on their principal web sites, any known major entry points, and any web page where substantial personal information is collected from the public. The privacy policy must state what information is being collected, why it is being collected, and how the agency will use the information. Privacy policies must be clearly labeled and easily accessed when an individual visits a web site.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.
21	<p><b>Is a privacy policy statement posted on the web site?</b></p> <p><b>Remediation Guidance:</b> If no, then <i>OMB M-99-18</i> is invoked. Agencies must post privacy policies on their principal web sites, any known major entry points, as well as any web pages where substantial personal information is collected from the public. The privacy policy must state what information is being collected, why it is being collected, and how the agency will use the information. Privacy policies must be clearly labeled and easily accessed when an individual visits a web site.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.
22	<p><b>Are web links posted anywhere on the web site?</b></p> <p><b>Remediation Guidance:</b> If no, then <i>OMB M-99-18</i> is invoked. Agencies must post privacy policies on their principal web sites, any known major entry points, as well as any web pages where substantial personal information is collected from the public. The privacy policy must state what information is being collected, why it is being collected, and how the agency will use the information. Privacy policies must be clearly labeled and easily accessed when an individual visits a web site.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
23	<p><b>Are cookies present on the web site?</b></p> <p>Note: If yes, identify types of cookies in the Comments column.</p> <p><b>Remediation Guidance:</b> If yes, persistent cookies are prohibited. Alternatively, session cookies are allowed as long as use of session cookies are indicated in the privacy policy statement, and the agency is able to demonstrate a valid need for use of these session cookies. Cookies will not knowingly be transferred to third parties unless explained in the Privacy and Security Statement.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.
24	<p><b>Does the web site have any information or pages directed at children?</b></p> <p><b>Remediation Guidance:</b> If yes, then the <i>Children's Online Privacy Protection Act (COPPA)</i>, <i>OMB M-00-13</i>, and <i>DLMS 9 Chapter 1500</i> are all invoked. Agency systems hosting web sites are mandated by OMB to comply with COPPA. This law places restrictions on the collection and use of information on any web site or online service directed to children and requires parental consent before any such collection and provides the parent with the right to see what is collected about his/her child and to restrict dissemination or use or further collection of any information about the child.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
25	<p><b>Does the web site collect PII from individuals?</b></p> <p>Note: If yes, identify what PII the system collects in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b>                      If yes, and data elements relating to United States citizens or Lawful Permanent Residents are checked under both the Identifier and Personal Information categories, then the <i>Privacy Act of 1974</i> is invoked. Agencies must meet all requirements of the Privacy Act listed under <i>5 U.S.C. 552a.(4)</i> as amended listed under "Records Maintained On Individuals."</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then the <i>HIPAA Privacy Rule, 67 FR 14775</i> may be invoked. Agencies should review this rule to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then the <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
26	<p><b>Does the web site share PII with internal or external parties of the Department?</b></p> <p>Note: If yes, specify with whom and for what purposes, and identify the data elements in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b>                      If yes and the information relates to United States citizens or Lawful Permanent Residents, then section (e) (6) of the Privacy Act is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, agencies must make reasonable efforts to ensure that such records are accurate, complete, timely, and relevant on each system for agency purposes. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the Act.</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then <i>HIPAA Privacy Rule, 67 FR 14775</i> may be invoked. Agencies should review these rules to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then <i>Gramm-Leach-Bliley Act (GLBA) of 1999 Pub. Law No. 106-102, 113 Stat. 1338 (1999)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.
27	<p><b>Are rules of conduct in place for access to PII on the website?</b></p> <p>Note: If yes, identify in the Comments column all categories of users with access to PII on the system, and for what purposes the PII is used.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Administrative Controls</b>					
<p>Note: This PIA Guide uses the terms "Administrative," "Technical," and "Physical" to refer to security control questions—terms that are used in several federal privacy laws when referencing security requirements. USCIS recognizes the slight difference in terminology used in this guide from those that are used in other documents such as the <i>National Institute of Standards and Technology (NIST) SP 800-26, Security Self-Assessment Guide for Information Technology Systems</i>.</p>					
28	<p><b>Has the system been authorized to process information?</b></p> <p><b>Remediation Guidance:</b> If no, then the system may be required as directed by <i>OMB Circular A-130</i> to complete an accreditation for each system. Agencies should engage in an assessment process that ensures technical security features are built into the life cycle of a system.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
29	<p><b>Have there been major changes (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire) to the system since it was last certified and accredited?</b></p> <p><b>Remediation Guidance:</b> If yes, then agencies are required by <i>OMB Circular A-130</i> to complete an update of the certification and accreditation for each system that has been modified. Agencies should engage in an assessment process that ensures existing technical security features are appropriate to the modified system.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
30	<p><b>Are security controls routinely reviewed?</b></p> <p><b>Remediation Guidance:</b> Security controls need to be routinely reviewed to ensure sustained effectiveness even when no changes to the system have occurred. <i>OMB Circular A-130</i> stipulates a system's security controls should be reviewed "when significant modifications are made to a system, but at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system."</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Administrative Controls</b>					
31	<p><b>Is there a system security plan for this system?</b></p> <p><b>Remediation Guidance:</b>                      The <i>Privacy Act of 1974</i> and <i>OMB Circular A-130</i> require procedures be in place for implementing administrative, technical, and physical security controls for systems containing a system of records. Agencies should develop a plan that demonstrates security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from NIST security guidance.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Sensitive System Security Plan, Jan 04
32	<p><b>Is there a contingency (or backup) plan for the system?</b></p> <p><b>Remediation Guidance:</b>                      The <i>Privacy Act of 1974</i> and <i>OMB Circular A-130</i> require procedures be in place for implementing a contingency plan for systems containing a system of records. Agencies should develop a plan that demonstrates contingency security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from NIST security guidance.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Y2K Contingency Plan Backup procedures controlled by IDMS and DOJ Security software ("TOP SECRET")
33	<p><b>Are files backed up regularly?</b></p> <p><b>Remediation Guidance:</b>  <i>OMB Circular A-130</i> requires procedures be in place for protecting data on systems in the event the system and the information it contains is attacked or rendered unavailable. Agencies should devise a method for backing up information contained on the system at regular intervals.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Administrative Controls</b>					
34	<p><b>Are the backup files stored offsite?</b></p> <p><b>Remediation Guidance:</b>  <i>OMB Circular A-130</i> requires procedures be in place for protecting data on systems in the event the system and the information it contains is attacked or rendered unavailable. Agencies should identify an alternative site for housing backup files.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
35	<p><b>Are there user manuals for the system?</b></p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
36	<p><b>Have personnel using the system been trained and made aware of their responsibilities for protecting personal information being collected and maintained?</b></p> <p><b>Remediation Guidance:</b>                      If no, <i>OMB Circular A-130</i> requires that each agency ensure the security of information contained on each system to include training of users and employees of security controls in place. Agencies should provide users with training of their roles and responsibilities for protecting PII collected and maintained on the system.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Levels of access are conferred by (1) PICS and (2) supervisory staff at local office
37	<p><b>Who will have access to the PII on the system?</b></p> <p>Note: Check all that apply in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Users <input checked="" type="checkbox"/> Administrators <input checked="" type="checkbox"/> Developers <input checked="" type="checkbox"/> Contractors
38	<p><b>Are methods in place to ensure least privilege (e.g., "need to know" and accountability)?</b></p> <p>Note: If yes, please specify method(s) in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Technical Controls</b>					
39	<p><b>Are technical controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system?</b></p> <p>Note: If yes, check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, <i>OMB Circular A-130</i> requires that each agency ensure the security of information contained on each system by implementing technical security controls. Agencies should devise administrative, technical, and physical controls for each system to protect the PII it contains.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>USCIS has established technical control requirements including the following controls:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> User ID</li> <li><input checked="" type="checkbox"/> Passwords</li> <li><input checked="" type="checkbox"/> Firewall</li> <li><input type="checkbox"/> Virtual Private Network (VPN)</li> <li><input type="checkbox"/> Encryption</li> <li><input type="checkbox"/> Intrusion Detection System (IDS)</li> <li><input type="checkbox"/> Common Access Cards (CAC)</li> <li><input type="checkbox"/> Smart Cards</li> <li><input type="checkbox"/> Biometrics</li> <li><input type="checkbox"/> Public Key Infrastructure (PKI)</li> </ul>
40	<p><b>Are the following password controls in place?</b></p> <p>Note: Check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, <i>OMB Circular A-130</i> requires that each agency ensure the security of information contained on each system. Agencies should implement one or more of the password controls for each system to protect the PII it contains.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Passwords expire after a set period of time.</li> <li><input type="checkbox"/> Accounts are locked after a set period of inactivity.</li> <li><input checked="" type="checkbox"/> Minimum length of passwords is eight characters.</li> <li><input checked="" type="checkbox"/> Passwords must be a combination of uppercase, lowercase, and special characters.</li> <li><input checked="" type="checkbox"/> Accounts are locked after a set number of incorrect attempts.</li> </ul> <p>USCIS has established password management security requirements</p>
41	<p><b>Is a process in place to monitor and respond to incidents?</b></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Physical Controls</b>					
42	<p><b>Are physical access controls in place?</b></p> <p>Note: If yes, check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, <i>OMB Circular A-130</i> requires that each agency ensure the security of information contained on each system by implementing technical security controls. Agencies should devise administrative, technical, and physical controls for each system to protect the PII it contains.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>USCIS controls include:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Guards</li> <li><input checked="" type="checkbox"/> Identification Badges</li> <li><input checked="" type="checkbox"/> Key Cards</li> <li><input type="checkbox"/> Cipher Locks</li> <li><input type="checkbox"/> Biometrics</li> <li><input type="checkbox"/> Closed Circuit TV (CCTV)</li> <li><input type="checkbox"/> Other _____</li> <li><input type="checkbox"/> Other _____</li> <li><input type="checkbox"/> Other _____</li> </ul>

**APPENDIX D – PIA QUESTIONNAIRE – MFAS**

**NOTE:** Based on current privacy regulation and guidance, the PIA should be performed on the production environment. For those systems that have test and development environments, those environments may or may not warrant their own Privacy Impact Assessment (PIA). The test and development environments (if generally do not necessitate a separate PIA, however, the assessor may need to consult internal or technology (IT) system policy guidance and/or his or her security officer and/or the Office of the Chief Information Officer (OCIO) to confirm such decisions. For those systems that have performed risk assessments and defined system boundaries and scope, the system characterization will likely be the same for both the risk assessment and the PIA. PIAs performed at the initiation of the system development lifecycle will require conducting additional PIA intervals stipulated by the security handbook and when significant changes occur to the system.

General PIA attempts to determine what kind of personal information is contained within a system, what is done with that information and how that information is protected. There are many requirements for systems containing personal information based on external, local state privacy law, regulations, and guidance. Information guidance provided gives users and a point for meeting compliance at a minimum. However, users should be informed and review that law. It should have updated existing provisions of the Privacy Act statute. The Privacy Officer can answer questions that do not have legal implications. The OCIO can answer questions related to technical, management and physical controls on the system and includes a copy of a classification or question and answers.

System Name:	United States Citizenship and Immigration Services (USCIS) Marriage Fraud Amendment Act System (MFAS)
System Environment (production, test, development, or other. If other, please explain):	Production
System Location (entity/contractor name of site, building, room, city, and state):	N/A
Activity/Purpose of System:	To track, process and report on applications for immigration benefits.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>System Characterization</b>					
1	<p>Does USCIS own the system?</p> <p>Note: If no, identify the system owner in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Owner: b(6)
2	<p>Does USCIS operate the system?</p> <p>Note: If no, identify the system operator in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3	<p>Identify in the Comments column the life-cycle phase of this system.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Initiation <input type="checkbox"/> Develop/Acquisition <input type="checkbox"/> Implementation <input checked="" type="checkbox"/> Operations/Maintenance <input type="checkbox"/> Disposal
4	<p>Is the system a stand-alone system (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire)?</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	<p>Is the system network-connected (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire)?</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
6	<p>Is the system a General Support System (GSS), Major Application (MA) or sensitive system (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire)?</p> <p>Note: If yes, identify whether the system is a GSS, MA or sensitive system in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Sensitive But Unclassified

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>System Characterization</b>					
7	<p><b>Does the system <i>contain</i> PII within any database(s), record(s), file(s) or document(s)?</b></p> <p>Note: If yes, check all that apply in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If the system contains no records with any data elements listed in the comments section, the system is not subject to federal privacy laws or regulations such as the <i>Privacy Act of 1974</i>. Questions 8-18 may be marked with an "N/A."</p> <p>If data elements relating to persons who are either United States Citizens or Lawful Permanent Residents are checked under the personal information category in the comments column, then the <i>Privacy Act of 1974</i> is invoked. Agencies must meet all requirements of the Privacy Act listed under 5 U.S.C. 552a.(4) as amended, listed under "Records Maintained On Individuals."</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then the <i>HIPAA Privacy Rule 67 FR 14775</i> may be invoked. Agencies should review this rule to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then the <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p><b>Personal Information:</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Name</li> <li><input checked="" type="checkbox"/> Date of Birth</li> <li><input checked="" type="checkbox"/> Social Security Number (or other number originated by a government that specifically identifies an individual)</li> <li><input type="checkbox"/> Photographic Identifiers (e.g., photograph image, x-rays, and video)</li> <li><input checked="" type="checkbox"/> Driver's License</li> <li><input type="checkbox"/> Biometric Identifiers (e.g., fingerprint and voiceprint)</li> <li><input checked="" type="checkbox"/> Mother's Maiden Name</li> <li><input type="checkbox"/> Vehicle Identifiers (e.g., license plates)</li> <li><input checked="" type="checkbox"/> Mailing Address</li> <li><input checked="" type="checkbox"/> Phone Numbers (e.g., phone, fax, and cell)</li> <li><input type="checkbox"/> Medical Records Numbers</li> <li><input type="checkbox"/> Medical Notes</li> <li><input checked="" type="checkbox"/> Financial Account Information and/or Numbers (e.g., checking account number and PINs)</li> <li><input checked="" type="checkbox"/> Certificates (e.g., birth, death, and marriage)</li> <li><input checked="" type="checkbox"/> Legal Documents or Notes (e.g., divorce decree, criminal records, or other)</li> <li><input type="checkbox"/> Device Identifiers (e.g., pacemaker, hearing aid, or other)</li> <li><input type="checkbox"/> Web URLs</li> <li><input type="checkbox"/> Email Address</li> <li><input type="checkbox"/> Education Records</li> <li><input checked="" type="checkbox"/> Other: Alien Number (A-Number)</li> </ul>

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>System Characterization</b>					
8	<p><b>Has a Privacy Act Systems of Records Notice (PARN) been published in the Federal Register?</b></p> <p><b>Remediation Guidance:</b> If no, and the system meets the definition of a System of Records, then the <i>Privacy Act of 1974</i> requirements are invoked. Agencies must develop a PARN and publish the notice in the Federal Register with appropriate specifications listed in <i>5 U.S.C. Section 552a</i> as amended.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Included in CLAIMS 3
9	<p><b>Have major changes (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire) to the system been made since publication of the PARN?</b></p> <p><b>Remediation Guidance:</b> If yes, then the <i>Privacy Act of 1974</i> requires that agencies publish in the Federal Register a notice of any, and all revisions to the existence and character of the system of records with appropriate specifications listed in <i>5 U.S.C. Section 552a</i> as amended.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	<p><b>Does the PARN address all required categories of information?</b></p> <p>Note: Check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, then the notice specifying the existence of the system of records will include all criteria listed in the Comments column.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> System Name <input type="checkbox"/> Security Classification <input type="checkbox"/> System Location <input type="checkbox"/> Categories of Individuals Covered by the System <input type="checkbox"/> Categories of Records in the System <input type="checkbox"/> Authority of Maintenance of the System <input type="checkbox"/> Purpose <input type="checkbox"/> Routine Uses of Records Maintained in the System <input type="checkbox"/> Disclosure to Consumer Reporting Agencies <input type="checkbox"/> Policies and Practices for Storing, Retrieving, Accessing, Retaining and Disposing of Records <input type="checkbox"/> System Manager(s) and Address <input type="checkbox"/> Notification Procedure <input type="checkbox"/> Record Access Procedure <input type="checkbox"/> Contesting Record Procedure <input type="checkbox"/> Record Source Categories <input type="checkbox"/> Systems Exempted From Certain Provisions of the Act

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
11	<p><b>Does the system collect PII from individuals?</b></p> <p>Note: If yes, identify the PII the system collects directly from individuals in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> Each agency maintaining system of records is required to collect information to the greatest extent practicable directly from the individual when information may result in adverse determinations about an individual's rights, benefits, and privileges under federal programs.</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then <i>HIPAA Privacy Rule 67 FR 14775</i> may be invoked. Agencies should review these rules to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p><b>Personal Information:</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Alien Registration Number</li> <li><input checked="" type="checkbox"/> Name</li> <li><input checked="" type="checkbox"/> Date of Birth</li> <li><input checked="" type="checkbox"/> Social Security Number (or other number originated by a government that specifically identifies an individual)</li> <li><input type="checkbox"/> Photographic Identifiers (e.g., photograph image, x-rays, and video)</li> <li><input type="checkbox"/> Driver's License</li> <li><input checked="" type="checkbox"/> Biometric Identifiers (e.g., fingerprint and voiceprint)</li> <li><input checked="" type="checkbox"/> Mother's Maiden Name</li> <li><input type="checkbox"/> Vehicle Identifiers (e.g., license plates)</li> <li><input checked="" type="checkbox"/> Mailing Address</li> <li><input checked="" type="checkbox"/> Phone Numbers (e.g., phone, fax, and cell)</li> <li><input type="checkbox"/> Medical Records Numbers</li> <li><input type="checkbox"/> Medical Notes</li> <li><input checked="" type="checkbox"/> Financial Account Information and/or Numbers (e.g., checking account number and PINs)</li> <li><input checked="" type="checkbox"/> Certificates (e.g., birth, death, and marriage)</li> <li><input checked="" type="checkbox"/> Legal Documents or Notes (e.g., divorce decree, criminal records, or other)</li> <li><input type="checkbox"/> Device Identifiers (e.g., pacemaker, hearing aid, or other)</li> <li><input type="checkbox"/> Web URLs</li> <li><input type="checkbox"/> E-mail Address</li> <li><input type="checkbox"/> Education Records</li> <li><input type="checkbox"/> Other: _____</li> </ul>

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
12	<p><b>Does the system collect PII from other sources (e.g., databases, websites, etc.)?</b></p> <p>Note: If yes, specify the source(s) and PII collected in the Comments column.</p> <p><b>Remediation Guidance:</b> If yes, then each agency is required to maintain records on systems that are used for making determinations about an individual with accuracy, relevance, timeliness, and completeness as reasonably necessary to assure fairness to the individual. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the <i>Privacy Act of 1974</i>.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
13	<p><b>Does the system populate data for other resources (i.e., do databases, web sites, or other resources rely on this system's data)?</b></p> <p>Note: If yes, specify resource(s) and purpose for each instance in the Comments column.</p> <p><b>Remediation Guidance:</b> If yes, then section (e) (6) of the <i>Privacy Act of 1974</i> is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, the agency must make reasonable efforts to assure that such records are accurate, complete, timely, and relevant on each system for agency purposes. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the Act.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
14	<p><b>Does the system <i>share</i> PII with internal or external parties of USCIS?</b></p> <p>Note: If yes, identify in the Comments column which data elements are shared. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If yes, then section (e) (6) of the <i>Privacy Act of 1974</i> is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, agencies must make reasonable efforts to ensure that such records are accurate, complete, timely, and relevant on each system for agency purposes. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the Act.</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then <i>HIPAA Privacy Rule, 67 FR 14775</i> may be invoked. Agencies should review these rules to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
15	<p><b>Are records on the system retrievable?</b></p> <p>Note: If yes, specify in the Comments column what method is used in retrieving the records (i.e., using a record number, name, social security number, or other data element or record locator methodology). If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If yes, then a system of records in which information relating to a United States citizen or Lawful Permanent Resident is retrieved using one or more of an individual's "identifying information" invokes <i>Privacy Act of 1974</i> requirements. All requirements under <i>5 U.S.C. of Section 552a</i> as amended must be met by an agency for this system.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
16	<p><b>Is there a notification process in place when changes occur (i.e., revisions to PII or when the system encounters a major change or is replaced) for alerting other resources dependent upon PII contained on this system?</b></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
17	<p><b>Are processes in place for periodic review of PII contained in the system to ensure it is timely, accurate, and relevant?</b></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Information Sharing Practices</b>					
18	<p><b>Are rules of conduct in place for access to PII on the system?</b></p> <p>Note: If yes, identify in the Comments column all users with access to PII on the system, and for what purposes they use the PII.</p> <p><b>Remediation Guidance:</b> If no, then Section (e)(9-10) of the <i>Privacy Act of 1974</i> is invoked to the extent that the system contains information relating to United States citizens or Lawful Permanent Residents. The Act requires rules of conduct for persons involved in the design, development, operations, or maintenance of a system's PII.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p><input checked="" type="checkbox"/> Users  <input checked="" type="checkbox"/> Administrators  <input checked="" type="checkbox"/> Developers  <input checked="" type="checkbox"/> Contractors</p> <p>For what purposes:  <input type="checkbox"/> _____  <input type="checkbox"/> _____  <input type="checkbox"/> _____  <input type="checkbox"/> _____  <input type="checkbox"/> _____</p> <p>All users listed will be subject to USCIS and Rules of Behavior</p>
19	<p><b>Does the system host a web site either as an Internet, an intranet, or both?</b></p> <p>Note: If yes, identify what type of site in the Comments column.</p> <p><b>Note: If no, check N/A for all subsequent questions in the "Web Site Host Question Sets" section and answer questions starting with the "Administrative Controls" section beginning with Question #28.</b></p> <p><b>Remediation Guidance:</b> If yes, then <i>OMB M-99-18</i> is invoked requiring that for every federal, public web site agencies include a privacy policy statement, even if the site does <i>not</i> collect any information and does not create a Privacy Act record.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
20	<p><b>Is the web site accessible by the public or other entities (i.e., contractors, third party administrators, state, or local agencies, etc.)?</b></p> <p><b>Remediation Guidance:</b> If yes, then <i>OMB M-99-18</i> is invoked. Agencies must post privacy policies on their principal web sites, any known major entry points, and any web page where substantial personal information is collected from the public. The privacy policy must state what information is being collected, why it is being collected, and how the agency will use the information. Privacy policies must be clearly labeled and easily accessed when an individual visits a web site.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.
21	<p><b>Is a privacy policy statement posted on the web site?</b></p> <p><b>Remediation Guidance:</b> If no, then <i>OMB M-99-18</i> is invoked. Agencies must post privacy policies on their principal web sites, any known major entry points, as well as any web pages where substantial personal information is collected from the public. The privacy policy must state what information is being collected, why it is being collected, and how the agency will use the information. Privacy policies must be clearly labeled and easily accessed when an individual visits a web site.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.
22	<p><b>Are web links posted anywhere on the web site?</b></p> <p><b>Remediation Guidance:</b> If no, then <i>OMB M-99-18</i> is invoked. Agencies must post privacy policies on their principal web sites, any known major entry points, as well as any web pages where substantial personal information is collected from the public. The privacy policy must state what information is being collected, why it is being collected, and how the agency will use the information. Privacy policies must be clearly labeled and easily accessed when an individual visits a web site.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
23	<p><b>Are cookies present on the web site?</b></p> <p>Note: If yes, identify types of cookies in the Comments column.</p> <p><b>Remediation Guidance:</b> If yes, persistent cookies are prohibited. Alternatively, session cookies are allowed as long as use of session cookies are indicated in the privacy policy statement, and the agency is able to demonstrate a valid need for use of these session cookies. Cookies will not knowingly be transferred to third parties unless explained in the Privacy and Security Statement.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.
24	<p><b>Does the web site have any information or pages directed at children?</b></p> <p><b>Remediation Guidance:</b> If yes, then the <i>Children's Online Privacy Protection Act (COPPA)</i>, <i>OMB M-00-13</i>, and <i>DLMS 9 Chapter 1500</i> are all invoked. Agency systems hosting web sites are mandated by OMB to comply with COPPA. This law places restrictions on the collection and use of information on any web site or online service directed to children and requires parental consent before any such collection and provides the parent with the right to see what is collected about his/her child and to restrict dissemination or use or further collection of any information about the child.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
25	<p><b>Does the web site <i>collect</i> PII from individuals?</b></p> <p>Note: If yes, identify what PII the system collects in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b>                      If yes, and data elements relating to United States citizens or Lawful Permanent Residents are checked under both the Identifier and Personal Information categories, then the <i>Privacy Act of 1974</i> is invoked. Agencies must meet all requirements of the Privacy Act listed under <i>5 U.S.C. 552a.(4)</i> as amended listed under "Records Maintained On Individuals."</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then the <i>HIPAA Privacy Rule, 67 FR 14775</i> may be invoked. Agencies should review this rule to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then the <i>Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Web Site Host</b>					
26	<p><b>Does the web site <i>share</i> PII with internal or external parties of the Department?</b></p> <p>Note: If yes, specify with whom and for what purposes, and identify the data elements in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.</p> <p><b>Remediation Guidance:</b> If yes and the information relates to United States citizens or Lawful Permanent Residents, then section (e) (6) of the Privacy Act is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, agencies must make reasonable efforts to ensure that such records are accurate, complete, timely, and relevant on each system for agency purposes. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the Act.</p> <p>If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then <i>HIPAA Privacy Rule, 67 FR 14775</i> may be invoked. Agencies should review these rules to determine exact applicability and compliance requirements.</p> <p>If personal information on the system contains Financial Account Information and/or Numbers, then <i>Gramm-Leach-Bliley Act (GLBA) of 1999 Pub. Law No. 106-102, 113 Stat. 1338 (1999)</i> privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.
27	<p><b>Are rules of conduct in place for access to PII on the website?</b></p> <p>Note: If yes, identify in the Comments column all categories of users with access to PII on the system, and for what purposes the PII is used.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	See Question 19 above.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Administrative Controls</b>					
<p><b>Note:</b> This PIA Guide uses the terms “Administrative,” “Technical,” and “Physical” to refer to security control questions—terms that are used in several federal privacy laws when referencing security requirements. USCIS recognizes the slight difference in terminology used in this guide from those that are used in other documents such as the <i>National Institute of Standards and Technology (NIST) SP 800-26, Security Self-Assessment Guide for Information Technology Systems</i>.</p>					
28	<p><b>Has the system been authorized to process information?</b></p> <p><b>Remediation Guidance:</b> If no, then the system may be required as directed by <i>OMB Circular A-130</i> to complete an accreditation for each system. Agencies should engage in an assessment process that ensures technical security features are built into the life cycle of a system.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
29	<p><b>Have there been major changes (as defined in Appendix A, “Glossary of Terms” of the PIA Questionnaire) to the system since it was last certified and accredited?</b></p> <p><b>Remediation Guidance:</b> If yes, then agencies are required by <i>OMB Circular A-130</i> to complete an update of the certification and accreditation for each system that has been modified. Agencies should engage in an assessment process that ensures existing technical security features are appropriate to the modified system.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
30	<p><b>Are security controls routinely reviewed?</b></p> <p><b>Remediation Guidance:</b> Security controls need to be routinely reviewed to ensure sustained effectiveness even when no changes to the system have occurred. <i>OMB Circular A-130</i> stipulates a system’s security controls should be reviewed “when significant modifications are made to a system, but at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system.”</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Administrative Controls</b>					
31	<p><b>Is there a system security plan for this system?</b></p> <p><b>Remediation Guidance:</b>                      The <i>Privacy Act of 1974</i> and <i>OMB Circular A-130</i> require procedures be in place for implementing administrative, technical, and physical security controls for systems containing a system of records. Agencies should develop a plan that demonstrates security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from NIST security guidance.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
32	<p><b>Is there a contingency (or backup) plan for the system?</b></p> <p><b>Remediation Guidance:</b>                      The <i>Privacy Act of 1974</i> and <i>OMB Circular A-130</i> require procedures be in place for implementing a contingency plan for systems containing a system of records. Agencies should develop a plan that demonstrates contingency security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from NIST security guidance.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
33	<p><b>Are files backed up regularly?</b></p> <p><b>Remediation Guidance:</b>  <i>OMB Circular A-130</i> requires procedures be in place for protecting data on systems in the event the system and the information it contains is attacked or rendered unavailable. Agencies should devise a method for backing up information contained on the system at regular intervals.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Daily backups are performed.

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Administrative Controls</b>					
34	<p><b>Are the backup files stored offsite?</b></p> <p><b>Remediation Guidance:</b>  <i>OMB Circular A-130</i> requires procedures be in place for protecting data on systems in the event the system and the information it contains is attacked or rendered unavailable. Agencies should identify an alternative site for housing backup files.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	DOJ is responsible
35	<p><b>Are there user manuals for the system?</b></p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
36	<p><b>Have personnel using the system been trained and made aware of their responsibilities for protecting personal information being collected and maintained?</b></p> <p><b>Remediation Guidance:</b>                      If no, <i>OMB Circular A-130</i> requires that each agency ensure the security of information contained on each system to include training of users and employees of security controls in place. Agencies should provide users with training of their roles and responsibilities for protecting PII collected and maintained on the system.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
37	<p><b>Who will have access to the PII on the system?</b></p> <p>Note: Check all that apply in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Users <input checked="" type="checkbox"/> Administrators <input checked="" type="checkbox"/> Developers <input checked="" type="checkbox"/> Contractors
38	<p><b>Are methods in place to ensure least privilege (e.g., "need to know" and accountability)?</b></p> <p>Note: If yes, please specify method(s) in the Comments column.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Technical Controls</b>					
39	<p><b>Are technical controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system?</b></p> <p>Note: If yes, check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, <i>OMB Circular A-130</i> requires that each agency ensure the security of information contained on each system by implementing technical security controls. Agencies should devise administrative, technical, and physical controls for each system to protect the PII it contains.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>USCIS has established technical control requirements including the following controls:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> User ID</li> <li><input checked="" type="checkbox"/> Passwords</li> <li><input checked="" type="checkbox"/> Firewall</li> <li><input type="checkbox"/> Virtual Private Network (VPN)</li> <li><input type="checkbox"/> Encryption</li> <li><input type="checkbox"/> Intrusion Detection System (IDS)</li> <li><input type="checkbox"/> Common Access Cards (CAC)</li> <li><input type="checkbox"/> Smart Cards</li> <li><input type="checkbox"/> Biometrics</li> <li><input type="checkbox"/> Public Key Infrastructure (PKI)</li> </ul>
40	<p><b>Are the following password controls in place?</b></p> <p>Note: Check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, <i>OMB Circular A-130</i> requires that each agency ensure the security of information contained on each system. Agencies should implement one or more of the password controls for each system to protect the PII it contains.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Passwords expire after a set period of time.</li> <li><input checked="" type="checkbox"/> Accounts are locked after a set period of inactivity.</li> <li><input type="checkbox"/> Minimum length of passwords is eight characters.</li> <li><input type="checkbox"/> Passwords must be a combination of uppercase, lowercase, and special characters.</li> <li><input checked="" type="checkbox"/> Accounts are locked after a set number of incorrect attempts.</li> </ul> <p>USCIS has established password management security requirements. MFAS will be phased out as the new system is deployed.</p>
41	<p><b>Is a process in place to monitor and respond to incidents?</b></p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
<b>Physical Controls</b>					
42	<p><b>Are physical access controls in place?</b></p> <p>Note: If yes, check all that apply in the Comments column.</p> <p><b>Remediation Guidance:</b> If no, <i>OMB Circular A-130</i> requires that each agency ensure the security of information contained on each system by implementing technical security controls. Agencies should devise administrative, technical, and physical controls for each system to protect the PII it contains.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>USCIS controls include:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Guards</li> <li><input checked="" type="checkbox"/> Identification Badges</li> <li><input checked="" type="checkbox"/> Key Cards</li> <li><input type="checkbox"/> Cipher Locks</li> <li><input type="checkbox"/> Biometrics</li> <li><input type="checkbox"/> Closed Circuit TV (CCTV)</li> <li><input type="checkbox"/> Other _____</li> <li><input type="checkbox"/> Other _____</li> <li><input type="checkbox"/> Other _____</li> </ul>

**APPENDIX E – INFORMATION SHARING DATA ELEMENTS**

No.	Release	System Acronym	System Name	Information Shared
1	2	ANSIR	Automated Nationwide System for Immigration Review	Case information
2	1	BCS	Background Check Service	Background check information
3	1	BRS	Biometric Repository System	Unified repository for all biometric data
4	1	CIA via BCS	Central Intelligence Agency System	Background information
5	1	CIS	Central Index System	Case history
6	1	CLAIMS 3 LAN	Computer Linked Application Information Management System (CLAIMS) 3 Local Area Network (LAN)	Case processing data
7	1	CLAIMS 3 Mainframe	Computer Linked Application Information Management System (CLAIMS) 3 Mainframe	Case processing data
8	1	CLAIMS 4	Computer Linked Application Information Management System (CLAIMS) 4	Case processing data for N-400 cases
9	3		Credit Check System	Credit history
10	1	DACS	Deportable Alien Control System	Deportation and detention information
11	2		Defense Investigative Service System	Background information
12	1	DCOS	Debt Collection System	Payment status
13	2		Department of Defense System	Background information
14	2		Department of Labor System	Labor certification
15	1	E-Filing	Electronic Filing	Benefit application information
16	2	EID/EREM	Enforcement Integrated Database/ Enforcement Removal Module	Deportation action
17	1	IAFIS via BCS	Integrated Automated Fingerprint Identification System (IAFIS)	Fingerprint biometrics
18	2	FBI via BCS	Federal Bureau of Investigation Name System	Criminal background
19	1		Fee Franking Machine	Form type

No.	Release	System Acronym	System Name	Information Shared
20	1	FFMS	Federal Financial Management System	Revenue and form type
21	2	FIPS	FOIA Information Processing System	Case information
22	1	IBIS via BCS	Interagency Border Inspection System	Background information
23	1	IDENT	Automated Biometric Fingerprint Identification System	Fingerprint biometrics
24	3		Internal Revenue Service System	Tax Returns, Wage and Tax Statement W-2
25	1	IVAMS	Immigration Visa Allocation Management System	Immigration visa availability
26	1	IVIS	Immigrant Visa Information Systems	Visa petition information
27	3	KM	Knowledge Management	
28	1		Lockbox	Benefit application/petition data; scanned applications, petitions, evidence (proposed)
29	1	NAILS	National Automated Immigration Lookout System	Background information
30	1	National Scheduler	National Scheduler (proposed)	Fingerprint, interview, oath ceremony schedule availability
31	2	Naturalization Testing System	Naturalization Testing System	Test Results
32	1	NCSC CRIS	National Customer Service Center Customer Relationship Interface System (includes Change of Address module)	Address change information Case Status Information
33	1	NCSC IVRS	National Customer Service Center Integrated Voice Response System	Case status
34	1	NFTS	National File Tracking System	Paper file location
35	1	NIIS	Nonimmigrant Information System	Arrival/Departure information; Change of Addresses information (AR-11 module)

No.	Release	System Acronym	System Name	Information Shared
36	1	NPS	National Production System	Integrated Card Production System (ICPS) jobs for Permanent Residency Cards, Employment Authorization Documents
37	2	RAPS	Refugee Asylum Processing System	Case history
38	1	RNACS	Reengineered Naturalization Application Casework System	Case processing data
39	TBD		Selective Service System	Selective Service registration verification
40	TDB	SEVIS	Student and Exchange Visitor Information System	Background information
41	TBD		Social Security Administration System	Social Security Number verification; income assistance information
42	2	U.S Visit	U.S Visit	Arrival/Departure information
43	TBD	WRAPS	Worldwide Refugee Admission Processing System	Background information

**APPENDIX F – USER ROLES**

User Roles	User Role Description
Headquarter Functional Administrator	This user is responsible for one or more forms that provide similar benefits, such as employment-based visas. This user is thoroughly knowledgeable of the process of these forms. In this capacity, this user is responsible for ensuring that the system's processing of the forms is in compliance with Federal Government laws, regulations and policies. Maintaining the form profiles is the primary means of accomplishing this task.
Super User	This is the user who is able to perform all functions within the Benefits Application Processing System (BAPS). This user's main responsibilities will be entailed of maintaining user profiles, office profiles, quality assurance profiles, maintaining forms, notices, exams, codes, user roles, permissions, Visa profiles. This user is created to be the key to test any issues that other users may encounter. Therefore, this user should have access to the complete set of system permissions or activities.
DO Management	This user is responsible for the management of their respective offices. Their duties include the administration of user profile, workload distribution among the office's users. These managers work with higher echelon management to control workload and processing changes.
SC Management	This user is responsible for the management of their respective offices. Their duties include the administration of user profile, workload distribution among the office's users. These managers work with higher echelon management to control workload and processing changes.
ASC Management	This user is responsible for the management of their respective offices. Their duties include the administration of user profile, workload distribution among the office's users. These managers work with higher echelon management to control workload and processing changes.
DO Data Entry (Clerks, Preadjudicative Team)	This individual records and process applications, verifies information, schedules interviews, exams, and oath ceremony appointments and sends notices to applicants. Data Entry team lead helps or monitors cases being prepared for adjudication.
SC Data Entry (Clerks, Preadjudicative Team)	This individual records and process applications, verifies information, schedules interviews, exams, and oath ceremony appointments and sends notices to applicants. Data Entry team lead helps or monitors cases being prepared for adjudication.
ASC Clerk	This individual is responsible for recording appointment results and reviewing case information.
DO System Administrator (ADP)	This user uses Ad-Hoc reports and standard reports to monitor and manage office workload.
SC System Administrator (ADP)	This user uses Ad-Hoc reports and standard reports to monitor and manage office workload.
ASC System Administrator (ADP)	This user uses Ad-Hoc reports and standard reports to monitor and manage office workload.
SC Officer	This user is primarily responsible for adjudicating cases.

User Roles	User Role Description
DO Officer	This user is primarily responsible for adjudicating cases.
Quality Assurance Personnel	This user reviews cases for information accuracy & quality and conducts case processing audits.
General User	<p>These roles are assigned to any user who requires read only access. This user is limited to searching, displaying and reviewing case information. The following user types can be assigned this role:</p> <ul style="list-style-type: none"> <li>• HQ Management;</li> <li>• AAU/BIA Staff;</li> <li>• EOIR;</li> <li>• Investigations (USCIS, BICE, BCBP);</li> <li>• NCSC;</li> <li>• National Record Center;</li> <li>• Debt Management Center;</li> <li>• LESC;</li> <li>• FOIA;</li> <li>• SAVE;</li> <li>• SSA;</li> <li>• CPAU;</li> <li>• CRU;</li> <li>• Others to be determined.</li> </ul>

**Attachment 6**  
**Biometrics Survey: US Coast Guard**

The US Coast Guard (USCG) collects biometrics for all License and Merchant Marine Document (MMD) applications and renewals. The following responses pertain to this program.

**Please identify the program/initiative and the purpose for using biometrics.**

Department of Justice Criminal History Check for all License and Merchant Marine Document (MMD) applications and renewals.

If positive hit, information is sent to local Officer-in-Charge of Marine Investigations (OCMI)/Regional Exam Center (REC) with Merchant Marine Security Services Branch (NMC-4D) recommended action.

**What is the type of biometrics technology used?**

Currently using FD258 Standard Finger Print Card.

Intend to implement Live Scan System (Cross Match Inc.): fingerprints will be electronically submitted for a quicker turnaround time.

**How much did it cost your agency to implement the use of biometrics for the program/initiative and what is the FY04 projected cost for using the technology?**

\$18.00 per card

\$620,000 budgeted for fingerprint card processing

Does not include civil service salary or contractor rate.

Does not include cost of Live Scan System

**Is the use of biometrics for this program or initiative mandated by statute or rule? If YES, reference the statutory or regulatory citation.**

46CFR10.201(h) (1-6) Criminal Record Review for all Licenses

46CFR12.02-4(c)(1-6) Criminal Record Review for Certification (MMD)

Commandant Instruction M16000.8B Marine Safety Manual; Volume III Marine Industrial Personnel; Chapter 8 Record Management for U.S. Merchant Mariners; A. Records Management; 10-Preparation of Fingerprint Records

**How is the biometrics information gathered, collected, and stored?**

Fingerprints (and duplicate) collected at 17 RECs; sent to the National Maritime Center (NMC) and forwarded to the Federal Bureau of Investigation (FBI).

Positive or Negative results reported by the FBI; cards destroyed by FBI. Duplicate

Fingerprint Cards kept on file at NMC in a locked cabinet and destroyed after two years.

**Is the information accessible by other agencies or other entities (including contractors, vendors, and state and local governments)?**

If requested (none to date).

**Please describe the security measures used to protect the biometric information that is gathered, including any limitations on accessing the information.**

DOJ Criminal Report mailed to local REC.  
Fingerprint Cards and Criminal Report at NMC kept in a locked cabinet until mailed or destroyed.

**Did your agency conduct any privacy assessments for this use of biometrics? If so, please attach copies of any relevant assessments.**

No. Merchant Marine Fingerprints taken by U.S. Coast Guard since 1936, prior to the Privacy Act of 1974.

**At what rate have false-positives been returned during the use of biometrics in this program?**

"The currently available data is insufficient to generate an accurate measurement of false positives."

**What is the process in place to ensure that there is not repeated false-positives in the system?**

NMC-4D, Merchant Mariner Security Services Branch investigates all positive Criminal Reports.

**Please provide a copy of any procedures or policies your agency has in place regarding the use of biometrics. If these procedures or policies are program or initiative specific, please indicate so.**

Agency: National Maritime Center

Contact: b(6)

Telephone: b(2), b(6)

E-mail: b(2), b(6)

# Code of Federal Regulations



46

Parts 1 to 40

Revised as of October 1, 2003

Shipping

TABLE 10.109—FEES—Continued

If you apply for—	And you need—		
	Evaluation— then the fee is—	Examination— then the fee is—	Issuance—then the fee is—
Renewal	No fee	No fee	No fee.

\* Duplicate for document lost as result of marine casualty—No Fee.

[USCG-1997-2799, 64 FR 42814, Aug. 5, 1999; 64 FR 53230, Oct. 1, 1999]

§ 10.110 Fee payment procedures.

- (a) You may pay—
  - (1) All fees required by this section when you submit your application; or
  - (2) A fee for each phase at the following times:
    - (i) An evaluation fee when you submit your application.
    - (ii) An examination fee before you take the first examination section.
    - (iii) An issuance fee before you receive your license or certificate of registry.
  - (b) If you take your examination someplace other than a Regional Examination Center (REC), you must pay the examination fee to the REC at least one week before your scheduled examination date.
    - (c) Unless the REC provides additional payment options, your fees may be paid as follows:
      - (1) Your fee payment must be for the exact amount.
      - (2) Make your check or money order payable to the U.S. Coast Guard, and write your social security number on the front of each check or money order.
      - (3) If you pay by mail, you must use either a check or money order.
      - (4) If you pay in person, you may pay with cash, check, or money order at Coast Guard units where Regional Examination Centers are located.
    - (d) Unless otherwise specified in this part, when two or more documents are processed on the same application—
      - (1) *Evaluation fees.* If a certificate of registry transaction is processed on the same application as a license transaction, only the license evaluation fee will be charged; and
      - (2) *Issuance fees.* A separate issuance fee will be charged for each document issued.

[USCG-1997-2799, 64 FR 42815, Aug. 5, 1999]

§ 10.111 Penalties.

- (a) Anyone who fails to pay a fee or charge established under this subpart is liable to the United States Government for a civil penalty of not more than \$5,000 for each violation.
  - (b) The Coast Guard may assess additional charges to anyone to recover collection and enforcement costs associated with delinquent payments of, or failure to pay, a fee. Coast Guard licensing services may also be withheld from anyone pending payment of outstanding fees owed to the Coast Guard for services already provided by Regional Examination Centers.

[CGD 91-002, 58 FR 15237, Mar. 19, 1993]

§ 10.112 No-fee license for certain applicants.

- (a) For the purpose of this section, a no-fee license applicant is a person who is a volunteer, or part-time or full-time employee of an organization which is:
  - (1) Charitable in nature;
  - (2) Not for profit; and
  - (3) Youth oriented.
- (b) An organization may submit a written request to Commanding Officer, U.S. Coast Guard National Maritime Center, 4200 Wilson Boulevard, Suite 630, Arlington, VA 22203-1804 in order to be considered an eligible organization under the criteria set forth in paragraph (a) of this section. With the written request, the organization must provide evidence of its status as a youth oriented, not for profit, charitable organization.

NOTE: The following organizations are accepted by the Coast Guard as meeting the requirements of paragraph (a) of this section and need not submit evidence of their status: Boy Scouts of America, Sea Explorer Association, Girl Scouts of the United States of America, and Young Men's Christian Association of the United States of America.

- (c) A letter from an organization determined eligible under paragraph (b) of this section must also accompany the person's license application to the Coast Guard. The letter must state that the purpose of the person's application is solely to further the conduct of the organization's maritime activities. The applicant then is eligible under this section to obtain a no-fee license if other requirements for the license are met.
  - (d) A marine license issued to a person under this section is endorsed restricting its use to vessels owned or operated by the sponsoring organization.
  - (e) The holder of a no-fee license issued under this section may have the restriction removed by paying the appropriate evaluation, examination, and issuance fees that would have otherwise applied.

[CGD 91-002, 58 FR 15238, Mar. 19, 1993, as amended by CGD 95-072, 60 FR 50460, Sept. 29, 1995; CGD 98-041, 61 FR 50726, Sept. 27, 1996; CGD 97-057, 62 FR 51042, Sept. 30, 1997; USCG-2001-10224, 66 FR 48619, Sept. 21, 2001]

Subpart B—General Requirements for All Licenses and Certificates of Registry

§ 10.201 Eligibility for licenses and certificates of registry, general.

- (a) Each applicant shall establish to the satisfaction of the OCMI that he or she possesses all of the qualifications necessary (such as age, experience, character references and recommendations, physical health or competence and test for dangerous drugs, citizenship, approved training, passage of a professional examination, as appropriate, and, when required by this part, a practical demonstration of skills) before the OCMI will issue a license or certificate of registry.
  - (b) No person who has been convicted by a court of record of a violation of the dangerous drug laws of the United States, the District of Columbia, or any State or territory of the United States is eligible for a license or certificate of registry, except as provided by the provisions of paragraph (h) of this section. No person who has ever been the user of, or addicted to the use of, a dangerous drug, or has ever been convicted of an offense described in

section 205 of the National Driver Register Act of 1982 (49 U.S.C. 30304) due to the addiction or abuse of alcohol is eligible for a license or certificate of registry unless he or she furnishes satisfactory evidence of suitability for service in the merchant marine as provided in paragraph (j) of this section.

- (c) Except as provided in § 10.464(i) of the part, an applicant for a license must demonstrate an ability to speak and understand English as found in the navigation rules, aids to navigation publications, emergency equipment instructions, machinery instructions, and radiotelephone communications instructions.
  - (d) An applicant for a license must meet the requirements for recent service specified in § 10.202(e).
  - (e) No license or certificate of registry may be issued to any person who is not a citizen of the United States with the exception of operator of uninspected passenger vessels limited to vessels not documented under the laws of the United States.
    - (f) Except as specified in this paragraph, no license or certificate of registry may be issued to a person who has not attained the age of 21 years.
      - (1) A license as master of near coastal, Great Lakes and inland, inland, or river vessels of 25-200 gross tons, third mate, third assistant engineer, mate of vessels of 200-1600 gross tons, ballast control operator, assistant engineer (MODU), assistant engineer of fishing industry vessels, mate (pilot) of towing vessels, radio officer, assistant engineer (limited-oceans), or designated duty engineer of vessels of not more than 4000 horsepower may be granted to an applicant who has reached the age of 19 years.
      - (2) A license as limited master of near coastal vessels of not more than 100 gross tons, limited master of Great Lakes and inland vessels of not more than 100 gross tons, mate of Great Lakes and inland vessels of 25-200 gross tons, mate of near coastal vessels of 25-200 gross tons, operator of uninspected passenger vessels, or designated duty engineer of vessels of not more than 1,000 horsepower, or apprentice mate (steersman) of towing vessels, may be granted to an applicant, otherwise

qualified, who has reached the age of 18 years.

(g) Persons serving or intending to serve in the merchant marine service are recommended to take the earliest opportunity of ascertaining, through examination, whether their visual acuity, and color vision where required, are such as to qualify them for service in that profession. Any physical impairment or medical condition which would render an applicant incompetent to perform the ordinary duties of an officer at sea is cause for denial of a license.

(h) *Criminal Record Review.* The OCMI may review the criminal record of an applicant for the issuance of a license or certificate of registry issued as an original or reissued with a new expiration date. An applicant conducting simultaneous merchant mariner's credential transactions shall undergo only one criminal record check. Applicants must provide written disclosure of all prior convictions at the time of application.

(1) If the applicant is advised that a criminal record check is required by the OCMI, applicants shall provide their fingerprints at the time of application. The fingerprints will be used to determine whether the applicant has a record of a criminal conviction. An application may be disapproved if a criminal record review leads the OCMI to determine that the applicant's habits of life and character are such that the applicant cannot be entrusted with the duties and responsibilities of the license or certificate of registry for which application is made. If an application is disapproved, the OCMI will notify the applicant in writing of the reason(s) for disapproval and advise the applicant that the reconsideration and appeal procedures in § 1.03 of this chapter apply. No examination will be given pending decision on appeal.

(2) The OCMI may use table 10.201(h) to evaluate applicants for licenses and certificates of registry who have criminal convictions. The table lists major categories of criminal activity and is not to be construed as an all-inclusive list. If an applicant is convicted of an offense that does not appear on the list, the OCMI will establish an appropriate assessment period using the list

as a guide. The assessment period commences when an applicant is no longer incarcerated. The applicant must establish proof of the time incarcerated and periods of probation and parole to the satisfaction of the OCMI. The assessment period may include supervised or unsupervised probation or parole. A conviction for a drug offense more than 10 years prior to the date of application will not alone be grounds for denial.

(3) When an applicant has convictions for more than one offense, the minimum assessment period will be the longest minimum in table 10.201(h) and table 10.201(i) based upon the applicant's convictions; the maximum assessment period will be the longest shown in table 10.201(h) and table 10.201(i) based upon the applicant's convictions.

(4) If a person with a criminal conviction applies for a license or certificate of registry before the minimum assessment period shown in table 10.201(h), or established by the OCMI under paragraph (h)(2) of this section has elapsed, then the applicant must provide evidence of suitability for service in the merchant marine. Factors which are evidence of suitability for service in the merchant marine are listed in paragraph (j) of this section. The OCMI will consider the applicant's evidence and may issue the license or certificate of registry in less than the listed minimum assessment period if the OCMI is satisfied that the applicant is suitable to hold the license or certificate of registry for which he or she has applied. If an applicant does not provide evidence of suitability for service in the merchant marine, then the application will be considered incomplete and will not be processed by the OCMI.

(5) If a person with a criminal conviction applies for a license or certificate of registry during the time between the minimum and maximum assessment periods shown in table 10.201(h) or established by the OCMI under paragraph (h)(2) of this section, the OCMI will consider the conviction and, unless there are offsetting factors, may grant the applicant the license or certificate of registry for which he or she has applied. Offsetting factors include multiple convictions, failure to comply

with court orders (e.g., child support orders), previous failures at rehabilitation or reform, inability to maintain steady employment, or any connection between the crime and the safe operation of a vessel. If the OCMI considers the applicant unsuitable for service in the merchant marine at the time of application, the OCMI will disapprove the application.

(6) If a person with a criminal conviction applies for a license or certificate of registry after the maximum assessment period shown in table 10.201(h) or established by the OCMI under paragraph (h)(2) of this section has elapsed,

then the OCMI will grant the applicant the license or certificate of registry for which he, or she has applied unless the OCMI has reason to believe the applicant is still unsuitable for service in the merchant marine. If the OCMI disapproves an application based upon a conviction older than the maximum assessment period, the OCMI will notify the applicant in writing of the reason(s) for the disapproval. The OCMI will also inform the applicant, in writing, that the reconsideration and appeal procedures contained in § 1.03 of this chapter apply.

TABLE 10.201(h)—GUIDELINES FOR EVALUATING APPLICANTS FOR LICENSES AND CERTIFICATES OF REGISTRY WHO HAVE CRIMINAL CONVICTIONS

Crime <sup>1</sup>	Assessment periods	
	Minimum	Maximum
<b>Crimes Against Persons<sup>2</sup></b>		
Homicide (intentional) .....	7 years .....	20 years.
Homicide (unintentional) .....	5 years .....	10 years.
Assault (aggravated) .....	5 years .....	10 years.
Assault (simple) .....	1 year .....	5 years.
Sexual Assault (rape, child molestation) .....	5 years .....	10 years.
Robbery .....	5 years .....	10 years.
Other crimes against persons <sup>2</sup> .		
<b>Crimes Against Property</b>		
Burglary .....	3 years .....	10 years.
Larceny (embezzlement) .....	3 years .....	5 years.
Other crimes against property <sup>2</sup> .		
<b>Vehicular Crimes</b>		
Conviction involving fatality .....	1 year .....	5 years.
Reckless Driving .....	1 year .....	2 years.
Racing on the Highways .....	1 year .....	2 years.
Other vehicular crimes <sup>2</sup> .		
<b>Crimes Against Public Safety</b>		
Destruction of Property .....	5 years .....	10 years.
Other crimes against public safety <sup>2</sup> .		
<b>Crimes Involving National Security</b>		
Terrorism, Acts of Sabotage, Espionage and related offenses .....	7 years .....	20 years.
<b>Criminal Violations of Environmental Laws</b>		
Criminal violations of environmental laws involving improper handling of pollutants or hazardous materials.	1 year .....	10 years.
<b>Dangerous Drug Offenses<sup>3,4,5</sup></b>		
Trafficking (sale, distribution, transfer) .....	5 years .....	10 years.
Dangerous drugs (Use or possession) .....	1 year .....	10 years.
Other dangerous drug convictions <sup>4</sup> .		

<sup>1</sup> Conviction of attempt, solicitation, aiding and abetting, accessory after the fact, and conspiracy to commit the criminal conduct listed in this table carry the same minimum and maximum assessment periods provided in the table.

<sup>2</sup> Other crimes are to be reviewed by the OCMI to determine the minimum and maximum assessment periods depending on the nature of the crime.

<sup>3</sup>Applicable only to original applications for licenses or CORs. Any applicant who has ever been the user of, or addicted to the use of, a dangerous drug shall meet the requirements of paragraph (b) of this section. Note: Applicants for reissue of a license or COR with a new expiration date, including a renewal or a raise of grade, who have been convicted of a dangerous drug offense while holding a license or COR, may have their applications withheld until appropriate action has been completed by the OCMI under the regulations which appear in 46 CFR part 5 governing administrative actions against merchant mariner credentials.

<sup>4</sup>The OCMI may consider dangerous drug convictions more than 10 years old only if there has been a dangerous drug conviction within the past 10 years.

<sup>5</sup>Applicants must demonstrate rehabilitation under paragraph (j) of this section, including applicants with dangerous drug use convictions more than ten years old.

<sup>6</sup>Other dangerous drug convictions are to be reviewed by the Officer in Charge, Marine Inspection on a case by case basis to determine the appropriate assessment periods depending on the nature of the offense.

(1) **National Driver Register.** A license or certificate of registry will not be issued as an original or reissued with a new expiration date unless the applicant consents to a check of the NDR for offenses described in section 205(a)(3) (A) or (B) of the NDR Act (i.e., operation of a motor vehicle while under the influence of, or impaired by, alcohol or a controlled substance; and any traffic violations arising in connection with a fatal traffic accident, reckless driving, or racing on the highways). The OCMI will not consider NDR listed civil convictions that are more than 3 years old from the date of request unless that information relates to the current suspension or revocation of the applicant's license to operate a motor vehicle. The OCMI may determine minimum and maximum assessment periods for NDR listed criminal convictions using table 10.201(h). An applicant conducting simultaneous merchant mariner's credential transactions is subject to only one NDR check.

(1) Any application may be disapproved if information from the NDR check leads the OCMI to determine that the applicant cannot be entrusted with the duties and responsibilities of the license or certificate of registry for which the application is made. If an application is disapproved, the OCMI will notify the applicant in writing of the reason(s) for disapproval and advise the application that the appeal procedures in §1.03 of this chapter apply. No examination will be given pending decision on appeal.

(2) Prior to disapproving an application because of information received from the NDR, the OCMI will make the information available to the applicant for review and written comment. The

applicant may submit records from the applicable State concerning driving record and convictions to the Coast Guard Regional Examination Center (REC) processing the application. The REC will hold an application with NDR listed convictions pending the completion of the evaluation and delivery by the individual of the underlying State records.

(3) The guidelines in table 10.201(i) will be used by the OCMI in evaluating applicants for licenses and certificates of registry who have drug or alcohol related NDR listed convictions. Non-drug or alcohol related NDR listed convictions will be evaluated by the OCMI under table 10.201(h) as applicable.

(4) An applicant may request an NDR file check for personal use in accordance with the Federal Privacy Act of 1974 (Pub. L. 93-579) by contacting the NDR at the following address: National Driver Register, Nassif Building, 400 7th Street, S.W., Washington, DC 20590.

(i) Applicants should request Form NDR-PRV or provide the following information on a notarized letter:

- (A) Full legal name;
- (B) Other names used;
- (C) Complete mailing address;
- (D) Driver license number;
- (E) Eye color;
- (F) Social security number;
- (G) Height;
- (H) Weight; and
- (I) Sex.

(ii) The NDR will respond to every valid inquiry including requests which produce no record(s) on the NDR file. Records can be made available, within a reasonable amount of time after the request, for personal inspection and copying during regular working hours at 7:45 a.m. to 4:15 p.m., each day except Federal holidays.

TABLE 10.201(i)—GUIDELINES FOR EVALUATING APPLICANTS FOR LICENSES AND CERTIFICATES OF REGISTRY WHO HAVE NDR MOTOR VEHICLE CONVICTIONS INVOLVING DANGEROUS DRUGS OR ALCOHOL<sup>1</sup>

No. of convictions	Date of conviction	Assessment period
1	Less than 1 year	1 year from date of conviction.
1	More than 1, less than 3 years	Application will be processed, unless suspension or revocation <sup>2</sup> is still in effect. Applicant will be advised that additional conviction(s) may jeopardize merchant mariner credentials.
1	More than 3 years old	Not necessary unless suspension or revocation is still in effect.
2 or more	Any less than 3 years old	1 year since last conviction and at least 3 years from 2nd most recent conviction, unless suspension or revocation is still in effect.
2 or more	All more than 3 years old	Application will be processed unless suspension or revocation is still in effect.

<sup>1</sup>Any applicant who has ever been the user of, or addicted to the use of, a dangerous drug shall meet the requirements of paragraph (b) of this section.

<sup>2</sup>Suspension or revocation, when referred to in table 10.201(i), means a State suspension or revocation of a motor vehicle operator's license.

(j) If an applicant has one or more alcohol or dangerous drug related criminal or NDR listed convictions; if the applicant has ever been the user of, or addicted to the use of, a dangerous drug; or if the applicant applies before the minimum assessment period for his or her conviction has elapsed; the OCMI may consider the following factors, as applicable, in assessing the applicant's suitability to hold a license or certificate of registry. This list is intended as a guide for the OCMI. The OCMI may consider other factors which he or she judges appropriate to a particular applicant, such as:

- (1) Proof of completion of an accredited alcohol- or drug-abuse rehabilitation program.
- (2) Active membership in a rehabilitation or counseling group, such as Alcoholics Anonymous or Narcotics Anonymous.
- (3) Character references from persons who can attest to the applicant's sobriety, reliability, and suitability for employment in the merchant marine including parole or probation officers.
- (4) Steady employment.
- (5) Successful completion of all conditions of parole or probation.

[CGD 81-059 and CGD 81-059a, 52 FR 38623 and 38666, Oct. 18, 1987, as amended by CGD 81-059, 54 FR 133, Jan. 4, 1989; CGD 81-059a, 55 FR 19799, Apr. 18, 1990; CGD 91-223, 60 FR 4524, Jan. 23, 1995; CGD 91-212, 60 FR 65484, Dec. 19, 1995; CGD 95-062, 62 FR 34529, June 26, 1997; USCG-1999-6224, 64 FR 63225, Nov. 19, 1999]

**§10.202 Issuance of licenses, certificates of registry, and STCW certificates or endorsements.**

(a) Applications for original licenses, original certificates of registry, raises of grade, extensions of route, or endorsements must be current and up-to-date with respect to service and the physical examination, as appropriate. Physical examinations and approved applications are valid for 12 months.

(b) Any person who is found qualified under the requirements set forth in this part is issued an appropriate license or certificate of registry valid for a term of 5 years from date of issuance. Any license or certificate of registry which is renewed or upgraded prior to its expiration date automatically becomes void upon issuance of the replacement license or certificate of registry.

(c) A license or certificate of registry is not valid until signed by the applicant and the OCMI (or the OCMI's designated representative).

(d) Every person who receives an original license or certificate of registry shall take an oath before a designated Coast Guard official that he or she will faithfully and honestly, according to his or her best skill and judgment, without concealment or reservation, perform all the duties required by law and obey all lawful orders of superior officers. Such an oath remains binding for all subsequent licenses or certificates of registry issued to that person unless specifically renounced in writing.

**National Driver Register (NDR)** means the nationwide repository of information on drivers maintained by the National Highway Traffic Safety Administration as provided under 49 U.S.C. Chapter 303.

**NDR listed convictions** means a conviction of any of the following motor vehicle-related offenses or comparable offenses:

(a) Operating a motor vehicle while under the influence of, or impaired by, alcohol or a controlled substance; or

(b) A traffic violation arising in connection with a fatal traffic accident, reckless driving, or racing on the highways.

**Original document** means the first merchant mariner's document issued to any person by the Coast Guard.

**Passes a chemical test for dangerous drugs** means the result of a chemical test conducted in accordance with 49 CFR part 40 is reported as "negative" by a Medical Review Officer in accordance with that part.

**Practical demonstration** means the performance of an activity under the direct observation of a designated examiner for the purpose of establishing that the performer is sufficiently proficient in a practical skill to meet a specified standard of competence or other objective criterion.

**Qualified instructor** means a person who has been trained or instructed in instructional techniques and is otherwise qualified to provide required training to candidates for licenses, documents, and endorsements. A faculty member employed or at a State maritime academy or the U.S. Merchant Marine Academy operated in accordance with 46 CFR part 310 and instructing in a navigation or engineering course is qualified to serve as a qualified instructor in his or her area(s) of specialization without individual evaluation by the Coast Guard.

**Qualified rating** means various categories of Able Seaman, Qualified Member of the Engine Department, Lifeboatman, or Tankerman endorsements on merchant mariner's documents.

**Standard of competence** means the level of proficiency to be achieved for

board vessels in accordance with national and international criteria.

**STCW** means the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978, as amended (incorporated by reference in § 12.01-3).

**STCW Code** means the Seafarer's Training, Certification and Watchkeeping Code.

**STCW endorsement** means a certificate or endorsement issued in accordance with STCW. An STCW endorsement issued by the Officer in Charge, Marine Inspection (OCMI), will be valid only when accompanied by the appropriate U.S. license or document; and, if the license or document is revoked, then the associated STCW endorsement will no longer be valid for any purpose. References to STCW placed on a U.S. license or merchant mariner's document will suffice as STCW endorsements for the mariner serving on a vessel operating exclusively on a domestic voyage (i.e., to and from U.S. ports or places subject to U.S. jurisdiction).

[CGD 91-002, 58 FR 15238, Mar. 19, 1993, as amended by CGD 91-223, 60 FR 4525, Jan. 23, 1995; CGD 91-212, 60 FR 65487, Dec. 19, 1995; CGD 95-062, 62 FR 34534, June 26, 1997; CGD 97-057, 62 FR 51042, Sept. 30, 1997; USCG-1999-5610; 67 FR 66068, Oct. 30, 2002.]

#### § 12.01-7 Regional Examination Centers.

Licensing and Certification functions are performed only by the Officer in Charge, Marine Inspection, at the following locations:

Boston, MA	Toledo, OH
New York, NY	San Pedro, CA
Baltimore, MD	San Francisco, CA
Charleston, SC	Seattle, WA
Miami, FL	Anchorage, AK
New Orleans, LA	Juneau, AK
Houston, TX	Honolulu, HI
Memphis, TN	Portland, OR
St. Louis, MO	

Where the term *Officer in Charge, Marine Inspection*, or *Marine Inspection Office* is used within the context of this part it is to mean that *Officer* or *Office* at one of the above listed locations.

[CGD 82-033, 47 FR 28679, July 1, 1982, as amended by CGD 91-002, 58 FR 15239, Mar. 19, 1993; USCG-2000-7790, 65 FR 58468, Sept. 29,

#### § 12.01-9 Paperwork approval.

(a) This section lists the control numbers assigned by the Office of Management and Budget under the Paperwork Reduction Act of 1980 (Pub. L. 96-511) for the reporting and record keeping requirements in this part.

(b) The following control numbers have been assigned to the sections indicated:

(1) OMB 2115-0624-46 CFR 12.02-17 and 12.03-1.

(2) [Reserved].

[CGD 95-062, 62 FR 34535, June 26, 1997]

#### Subpart 12.02—General Requirements for Certification

##### § 12.02-3 Where documents are issued.

(a) Certificates of identification, certificates of service, certificates of efficiency, and continuous discharge books are issued to applicants qualifying therefor at any Marine Inspection Office of the Coast Guard during usual business hours.

(b)(1) Coast Guard Merchant Marine Details abroad are authorized to conduct examinations for upgrading of seamen, but are not prepared to conduct the physical examination where required. Merchant Marine Details will therefore not issue regular certificates, but temporary permits in lieu thereof. Merchant Marine Details will instruct the recipient of each temporary permit to present it to the Officer in Charge, Marine Inspection, upon arrival in the first port in the United States in which a Marine Inspection Office is located in order to exchange it for a permanent certificate.

(2) The temporary permit shall be accepted in a Marine Inspection Office as proof that the bearer has complied with the rules and regulations governing the issuance of certificates, except as noted in the body of the temporary permit. The requirements noted in the exceptions will be complied with as in the case of other applicants.

(3) The written examinations are forwarded to the Commanding Officer, National Maritime Center by Merchant Marine Details, and any Marine Inspection Office at which an applicant with a temporary permit appears may request and obtain the examination in

the case from the Commanding Officer National Maritime Center. Any Marine Inspection Office which doubts the propriety of issuing a permanent certificate in lieu of a temporary permit which has been issued by a foreign Merchant Marine Detail shall inform the Commanding Officer, National Maritime Center fully as to the circumstances.

[CGFR 65-50, 30 FR 16640, Dec. 30, 1965, as amended by CGD 95-072, 60 FR 50460, Sept. 29, 1995; USCG-1998-4442; 63 FR 52189, Sept. 30, 1998]

##### § 12.02-4 Basis for denial of documents.

(a) No person who has been convicted by a court of record of a violation of the dangerous drug laws of the United States, the District of Columbia, or any State or territory of the United States is eligible for an original merchant mariner's document, except as provided by the provisions of paragraph (c) of this section. No person who has ever been the user of, or addicted to the use of, a dangerous drug, or has ever been convicted of an offense described in section 205 of the National Driver Register Act of 1982 (49 U.S.C. 30304) due to the addiction or abuse of alcohol is eligible for a merchant mariner's document unless he or she furnishes satisfactory evidence of suitability for service in the merchant marine as provided in paragraph (e) of this section.

(b) An applicant who fails a chemical test for dangerous drugs required by § 12.02-9 will not be issued a merchant mariner's document.

(c) **Criminal Record Review.** The Officer in Charge, Marine Inspection, may require a criminal record check of an applicant for a merchant mariner's document issued as an original or reissued with a new expiration date. An applicant conducting simultaneous merchant mariner's credential transactions shall undergo only one criminal record check. Applicants must provide written disclosure of all prior convictions at the time of application.

(1) If a criminal record check is required by the Officer in Charge, Marine Inspection, applicants shall provide fingerprints at the time of application

The fingerprints will be used to determine whether the applicant has a record of a criminal conviction. An application may be disapproved if the individual's criminal record leads the Officer in Charge, Marine Inspection to determine that the applicant cannot be entrusted with the duties and responsibilities of the merchant mariner's document for which application is made. If an application is disapproved, the Officer in Charge, Marine Inspection will notify the applicant in writing of the reason(s) for disapproval and advise the applicant that the appeal procedures in § 1.03 of this chapter apply. No examination will be given pending decision on appeal.

(2) The Officer in Charge, Marine Inspection will use table 12.02-4(c) to evaluate applicants for merchant mariner's documents who have criminal convictions. The table lists major categories of criminal activity and is not to be construed as an all-inclusive list. If an applicant is convicted of an offense that does not appear on the list, the Officer in Charge, Marine Inspection will establish an appropriate assessment period using the list as a guide. The assessment period commences when an applicant is no longer incarcerated. The applicant must establish proof of the time incarcerated and periods of probation and parole to the satisfaction of the Officer in Charge, Marine Inspection. The assessment period may include supervised or unsupervised probation or parole. A conviction for a drug offense more than 10 years prior to the date of application will not alone be grounds for denial.

(3) When an applicant has convictions for more than one offense, the minimum assessment period will be the longest minimum in table 12.02-4(c) and table 12.02-4(d) based upon the applicant's convictions; the maximum assessment period will be the longest shown in table 12.02-4(c) and table 12.02-4(d) based upon the applicant's convictions.

(4) If a person with a criminal conviction applies for a merchant mariner's document before the minimum assessment period shown in table 12.02-4(c), or established by the Officer in Charge, Marine Inspection under paragraph (c)(2) of this section has elapsed, then

the applicant must provide, as part of the application package, evidence of suitability for service in the merchant marine. Factors which are evidence of suitability for service in the merchant marine are listed in paragraph (e) of this section. The Officer in Charge, Marine Inspection will consider the applicant's evidence submitted with the application and may issue the merchant mariner's document in less than the listed minimum assessment period if the Officer in Charge, Marine Inspection is satisfied that the applicant is suitable to hold the merchant mariner's document for which he or she has applied. If an application filed before the minimum assessment period has elapsed does not include evidence of suitability for service in the merchant marine, then the application will be considered incomplete and will not be processed by the Officer in Charge, Marine Inspection until the applicant provides the necessary evidence as set forth in paragraph (e) of this section.

(5) If a person with a criminal conviction applies for a merchant mariner's document during the time between the minimum and maximum assessment periods shown in table 12.02-4(c) or established by the Officer in Charge, Marine Inspection under paragraph (c)(2) of this section, then the Officer in Charge, Marine Inspection shall consider the conviction and, unless there are offsetting factors, shall grant the applicant the merchant mariner's document for which he or she has applied. Offsetting factors include such factors as multiple convictions, failure to comply with court orders (e.g., child support orders), previous failures at rehabilitation or reform, inability to maintain steady employment, or any connection between the crime and the safe operation of a vessel. If the Officer in Charge, Marine Inspection considers the applicant unsuitable for service in the merchant marine at the time of application, the Officer in Charge, Marine Inspection may disapprove the application.

(6) If a person with a criminal conviction applies for a merchant mariner's document after the maximum assessment period shown in table 12.02-4(c) or established by the Officer in Charge, Marine Inspection under paragraph

(c)(2) of this section has elapsed, then the Officer in Charge, Marine Inspection will grant the applicant the merchant mariner's document for which he or she has applied unless the Officer in Charge, Marine Inspection considers the applicant still unsuitable for service in the merchant marine. If the Officer in Charge, Marine Inspection disapproves an applicant with a conviction older than the maximum assessment period listed in table 12.02-4(c),

the Officer in Charge, Marine Inspection will notify the applicant in writing of the reason(s) for the disapproval including the Officer in Charge, Marine Inspection's reason(s) for considering a conviction older than the maximum assessment period listed in table 12.02-4(c). The Officer in Charge, Marine Inspection will also inform the applicant, in writing, that the reconsideration and appeal procedures contained in § 1.03 of this chapter apply.

TABLE 12.02-4(c)—GUIDELINES FOR EVALUATING APPLICANTS FOR MERCHANT MARINER'S DOCUMENTS WHO HAVE CRIMINAL CONVICTIONS

Crime <sup>1</sup>	Assessment periods <sup>2</sup>	
	Minimum	Maximum
<b>Crimes Against Persons</b>		
Homicide (intentional) .....	7 years .....	20 years.
Homicide (unintentional) .....	5 years .....	10 years.
Assault (aggravated) .....	5 years .....	10 years.
Assault (simple) .....	1 year .....	5 years.
Sexual Assault (rape, child molestation) .....	5 years .....	10 years.
Other crimes against persons <sup>3</sup> .		
<b>Vehicular Crimes</b>		
Conviction involving fatality .....	1 year .....	5 years.
Reckless Driving .....	1 year .....	2 years.
Racing on the Highway .....	1 year .....	2 years.
Other vehicular crimes <sup>4</sup> .		
<b>Crimes Against Public Safety</b>		
Destruction of Property .....	5 years .....	10 years.
Other crimes against public safety <sup>5</sup> .		
<b>Crimes Involving National Security</b>		
Terrorism, Acts of Sabotage, Espionage and related offenses .....	7 years .....	20 years.
<b>Dangerous Drug Offenses<sup>3,4,5</sup></b>		
Trafficking (sale, distribution, transfer) .....	5 years .....	10 years.
Dangerous drugs (Use or possession) .....	1 year .....	10 years.
Other dangerous drug convictions <sup>6</sup> .		

<sup>1</sup> Conviction of attempts, solicitations, aiding and abetting, accessory after the fact, and conspiracies to commit the criminal conduct listed in this table carry the same minimum and maximum assessment periods provided in the table.

<sup>2</sup> Other crimes are to be reviewed by the Officer in Charge, Marine Inspection to determine the minimum and maximum assessment periods depending on the nature of the crime.

<sup>3</sup> Applicable to original applications only. Any applicant who has ever been the user of, or addicted to the use of, a dangerous drug shall meet the requirements of paragraph (a) of this section. Note: Applicants for reissue of a merchant mariner's document with a new expiration date including a renewal or additional endorsement(s), who have been convicted of a dangerous drug offense while holding a merchant mariner's document, may have their application withheld until appropriate action has been completed by the Officer in Charge, Marine Inspection under the regulations which appear in 46 CFR part 5 governing the administrative actions against merchant mariner credentials.

<sup>4</sup> The OCGM may consider dangerous drug convictions more than 10 years old only if there has been a dangerous drug conviction within the past 10 years.

<sup>5</sup> Applicants must demonstrate rehabilitation under paragraph (e) of this section, including applicants with dangerous drug use convictions more than ten years old.

<sup>6</sup> Other dangerous drug convictions are to be reviewed by the Officer in Charge, Marine Inspection on a case by case basis to determine the appropriate assessment period depending on the nature of the offense.

(d) *National Driver Register.* A merchant mariner's document will not be issued or reissued with a new expiration date unless the applicant consents

to a check of the NDR for offenses described in section 205(a)(3)(A) or (B) of the NDR Act (i.e., operation of a motor vehicle while under the influence of, or

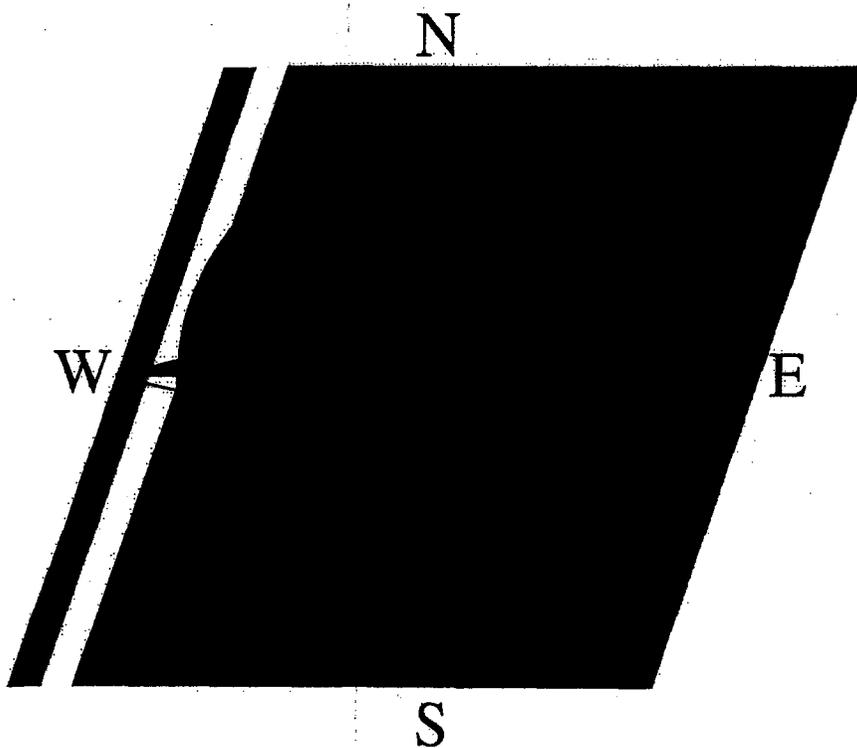
# MARINE SAFETY MANUAL

Volume III

MARINE INDUSTRY PERSONNEL

---

U.S. Department  
of Transportation  
**United States  
Coast Guard**



COMDTINST M16000.8B

# MARINE SAFETY MANUAL

## CHAPTER 8: RECORD MANAGEMENT FOR U.S. MERCHANT MARINERS

A. Records Management.....	8-1
1. Merchant Mariner's Document (MMD)/Sea Service Files.....	8-1
2. License And Certificate Records.....	8-1
3. Security Of Coast Guard Forms.....	8-1
4. License Stubs.....	8-2
5. Exam Room Logs.....	8-2
6. Transferring Seaman's Files Between RECs.....	8-2
7. Freedom Of Information Act Requests (FOIA).....	8-2
a. Non-Releasable Information.....	8-2
b. Releasable Information.....	8-3
c. FOIA Requests.....	8-3
8. Shipping Articles.....	8-3
9. Official Logbooks.....	8-3
10. Preparation Of Fingerprint Records.....	8-3
a. Applicant Fingerprint, Form FD-258.....	8-4
b. Authenticity Of Information.....	8-4
c. Radio Officers.....	8-5
d. Questionnaire for National Security Positions SF-86 (formally Coast Guard Intelligence Agency Check Request, Form CG-2765).....	8-5
B. License Information System (LIS).....	8-5

## MARINE SAFETY MANUAL

### CHAPTER 8: RECORD MANAGEMENT FOR U.S. MERCHANT MARINERS

#### A. Records Management.

This section provides guidance on the maintenance of license, certificate of registry, STCW certificates and document files by Regional Examination Centers (RECs). Additional guidance can be found in COMDTINST M5212.12, Paperwork Management Manual.

##### 1. Merchant Mariner's Document (MMD)/Sea Service Files.

Seamen documentation files are held at the REC for a period of one year from the date of the last transaction and then destroyed. All original applications shall be forwarded to Commanding Officer, National Maritime Center (NMC-4A) at the time the document is issued. When license and MMD transactions are completed at the same time, on the same application, the original application should be retained in the license file at the Regional Examination Center (REC) and a copy sent NMC-4A with a note that the original application is at the REC.

##### 2. License And Certificate Records.

Files should be sent to the Federal Records Center (FRC) seven years after the last transaction, e.g., license renewal, upgrade, and should first be sanitized by removing examination answer sheets and other extraneous material. The following are examples of file contents that should be forwarded to the FRC:

- a. Applications and all supporting documents;
- b. Letters of service;
- c. Records of examinations; and
- d. Canceled license(s) and STCW certificates, if the mariner does not want them.  
Return the canceled license(s) and STCW certificates to the mariner when possible.

##### 3. Security Of Coast Guard Forms.

Each REC shall maintain a record of licenses and Certificates of Registry forms, Certificates of Discharge (Form CG-718A), and all other controlled forms. Each REC shall maintain a log indicating who received the forms at the REC, the individual who received the forms for use, the date distributed for use, and signature of the recipient. Before signing the receipt, the custodian shall carefully check the control numbers of the documents being delivered to determine that none are missing. The bulk supply on hand should be securely packaged, kept in a safe or locked cabinet at all times, and periodically reviewed. The available supply for day-to-day use shall be checked daily against the control record. If at any time blank license/Certificate of Registry forms, Certificates of Discharge, or other controlled forms are discovered missing a unit investigation shall begin immediately. A complete report of the circumstances shall be made promptly following the investigation to Commanding Officer, National Maritime Center (NMC-4A), via the district commander. A complete audit of all blank forms should be completed:

- a. Semiannually;
- b. When staff members with access to the forms change; and
- c. At any other time the OCMI deems it necessary.

4. License Stubs.

These records are to be maintained at the REC for a period of seven years, then destroyed at the REC.

5. Exam Room Logs.

These logs should be retained one year then destroyed at the REC.

6. Transferring Seaman's Files Between RECs.

Files shall be forwarded by rapidraft letter requesting a receipt signature. The rapidraft should indicate who requested the file be transferred *and* how the request was made, e.g., phone, E-mail, letter. The file should be certified mail, return receipt requested. The originating REC will place the rapidraft and the signed return receipt in the now empty mariner's file folder. The contents of mariners' files may be transferred on a telephone request from the applicant or another REC.

7. Freedom Of Information Act Requests (FOIA).

When determining what information is releasable from a mariner's file under the Freedom of Information Act (FOIA), use the FOIA Manual, COMDTINST M5260.2, the FOIA officer, and the district legal staff. Be conservative in your determination, as additional items may be released under appeal; however, the file's custodian may be held personally accountable for violations of the mariner's privacy. Note that FOIA denials can only be made by designated officials, normally the district commander.

a. Non-Releasable Information.

(1) The following information must be withheld under exemption (b)(3) in 5 U.S.C. 552 because it is required by other statutes to be protected:

- (a) The fact that the mariner holds an MMD; and
- (b) All information contained on the Merchant Mariner's Document, Merchant Mariner's Document application or in the MMD record (manual or electronic). Forward all requests for information in MMD records to Commanding Officer, National Maritime Center (NMC-4A).

(2) The following information must be withheld under exemption (b)(6) in 5 U.S.C. 552 as a clearly unwarranted invasion of personal privacy:

- (a) Information regarding the arrest and conviction record, including Section IV, Narcotics Record of the License/MMD application, Form CG-719B and answers to the questions in blocks 20 and 21 of the old license application, Form CG-866;
- (b) Exam scores and employment records, including lists of discharges and letters of service as well as employment history listed on the application; and
- (c) Present address and home phone number.

b. Releasable Information.

- (1) Type and grade of license and certificate of registry, including endorsements.
- (2) Issue number.
- (3) Date and port of issue.

c. FOIA Requests.

Requests must be in writing, even if the only information desired is that which is on the face of the license.

8. Shipping Articles.

Shipping articles are submitted to Commanding Officer, National Maritime Center (NMC-4A) for review and filing. The shipping articles are maintained at Commanding Officer, National Maritime Center (NMC-4A) for three years then transferred to the FRC in Suitland, MD for an additional 60 years.

9. Official Logbooks.

The Official Logbooks are permanent records. They are submitted to the nearest OCMI for review by the Investigation Department, maintained at the Marine Safety Office for six months, then transferred to the nearest FRC for 60 years. After 60 years the Official Logbooks are sent to the National Archives Regional Center for permanent storage. A record of all official logbooks and their location must be maintained by the submitting office.

10. Preparation Of Fingerprint Records.

To comply with FBI policy and procedures governing criminal record checks, a classifiable form FD-258, Fingerprint Card, must be submitted for an original license, certificate of registry, Merchant Mariner's Document and 10% of renewable licenses/MMDs and new endorsements of licenses and MMDs. Only one set of fingerprint cards needs to be submitted when the applicant applies for a license and a Merchant Mariner's Document at the same time or within 6 months of a previous application. The REC should keep a second fingerprint card on file for one year to submit in case the first fingerprint card is rejected. Particular attention must be given to obtaining legible prints. The majority of rejections are due to one or more fingers not being rolled fully, the charts being smeared as the finger is being removed from the chart, or use of too much or too little ink. Any fingerprint that is smudged or otherwise illegible will be rejected. In addition, the FBI's system will reject any card containing any discrepancy which may include a blank entry or even a middle initial inserted in the place of a full middle name. The form FD-258 must have the proper ORI code number DCCG 00000, US COAST GUARD, WASH DC. A supply of form FD-258 with the proper code may be obtained by calling Commandant (NMC-4A). Fingerprint Cards, form FD-258, shall be submitted to Commanding Officer, National Maritime Center (NMC-4A) a minimum of once each week.

a. Applicant Fingerprint, Form FD-258.

To obtain the needed information for a criminal record check, compliance with the instructions on the back of form FD-258 is essential. Personnel must ensure that the following information is provided, either typed or legibly printed in blue or black ink.

- (1) Applicant's Name. (First, Middle, Last, Suffix)
- (2) Social Security Number.
- (3) Date of Birth.
- (4) Place of Birth.
- (5) Your No. OCA. This block must be completed with the alpha code for each REC and the applicant's social security number. The fingerprint card can NOT be processed without this code. The alpha codes are as follows:

A - Anchorage	T - Memphis
B - Baltimore	M - Miami
D - Boston	N - New Orleans
C - Charleston	Y - New York
G - Guam	P - Portland
I - Honolulu	F - San Francisco
H - Houston	S - San Juan
J - Juneau	W - Seattle
K - Ketchikan	L - St. Louis
E - Los Angeles/Long Beach	O - Toledo

EXAMPLE: For Memphis, OCA Block would read: T123456789

- (6) REC Location. The space entitled "Employer and Address" should contain the name and address of the Regional Examination Center where the application is submitted.
- (7) Reason For Fingerprinting. The reason for fingerprinting (original license, license as radio officer, certificate of registry as staff officer or MMD) must be typed or legibly printed in the space designated "Reason Fingerprinted."
- (8) Race. The space for "Race" will be completed with one of the following abbreviations only:

AI - American Indian	AN - Alaskan Native
A - Asian	PI - Pacific Islander
B - Black	H - Hispanic
W - White	

b. Authenticity Of Information.

If for any reason you doubt the information provided by the applicant, a letter stating the basis for doubt (including all pertinent details and justification) shall be referred to Commanding Officer, National Maritime Center (NMC-4A) for decision.

c. Radio Officers.

When an applicant has been approved for a license as radio officer and subsequently, within the five year renewal period, applies for an original MMD endorsed "See License as Radio Officer," a second set of fingerprints need not be obtained or submitted to the Commandant.

d. Questionnaire for National Security Positions SF-86 (formally Coast Guard Intelligence Agency Check Request, Form CG-2765).

Form SF-86, Questionnaire for National Security Positions, replaces the previous form CG-2765. The SF-86 must be executed for all non-U.S. citizens born outside the U. S., attached to the application and fingerprint forms, and forwarded to Commanding Officer, National Maritime Center. The NMC will forward the completed SF-86 to Immigration and Naturalization Service for processing and verification of an alien's legal entry into the U.S. Form SF-86 is available on Form Filler. Paper copies may be ordered from regular supply sources.

The applicant must complete Parts 1-14 (page #s 1-5), and sign the bottom of page 9. In addition, page 10 (Authorization For Release Of Information), must also be completed and signed.

B. License Information System (LIS).

All license, COR, and MMD transactions are now recorded in a central computer system, the Merchant Mariner Licensing and Documentation System (MMLD). Therefore, LIS cards are no longer used.

INTERNATIONAL LABOUR OFFICE  
BUREAU INTERNATIONAL DU TRAVAIL  
OFICINA INTERNACIONAL DEL TRABAJO

4, route des Morillons, CH-1211 GENEVE 22  
Telephone +4122 799 61 11 Fac-simile +4122 799 86 85 E-mail: [ilo@ilo.org](mailto:ilo@ilo.org)  
Telegramme INTERLAB GENEVE

**Biometric Profile for Minutiae-Based Seafarers' Identity Documents**

Source: Project Editors

Revision History

Revision	Date	Document Number	Comments
0.0	2004-01-16	ILO SID-0002	First Draft

Editors:



**Contents**

	Page
Forward.....	3
0 Introduction .....	5
0.1 Rationale for document development.....	5
0.2 Related efforts.....	5
1 Scope.....	7
2 Conformance .....	8
3 References.....	8
3.1 Conformative standards .....	8
3.2 Informative references .....	9
3.3 Additional standards and documentation to be developed.....	9
4 Terms and definitions.....	10
4.1 Terms and definitions.....	10
5 SID biometric requirements.....	12
5.1 SID minutiae-based fingerprint biometric requirements .....	12
5.2 SID barcode requirements .....	15
5.3 SID identity verification requirements.....	17
5.4 SID database requirements .....	18
Annex A: SID Minutiae-Based Fingerprint Barcode Format.....	21
Annex B: SID Minutiae-Based Fingerprint Barcode Storage Format .....	22
Annex C - draft standard ISO 19794-2 .....	25
Annex D - draft standard ISO 19794-4 .....	63

## Forward

The International Labour Organization, established in 1919, is a Specialized Agency of the United Nations (UN). It is a tripartite organization, in which representatives of Governments, Employers and Workers take part with equal status. In June 2003, the ILO adopted the Seafarers' Identity Documents Convention (Revised), 2003 (Convention No. 185). The revision of the earlier Convention of 1958 was prompted by discussions held in the International Maritime Organization (IMO), reviewing measures and procedures to prevent acts of terrorism which threaten the security of passengers and crews and the safety of ships. The new ILO Convention has now been communicated to the Governments of ILO Members for their consideration with a view to ratification. It will become binding, as an international treaty, on all Members that ratify it.

The International Labour Office (the secretariat of the Organization) has commissioned the authors of this document to prepare a draft Technical Report to serve as a basis for a standard, to be later submitted to ISO with a view to endorsement, for an interoperable biometric template as required by Convention No. 185, covering fingerprint data capture, template generation, and barcode storage. The Report should refer to the most appropriate print technology, reader technology, enrolment procedures, barcode format, biometric sensors/readers, database considerations, and a global interoperable biometric template format. The report should also take into account database issues concerning quality and interoperability.

The authors submit this draft biometric profile to the ILO as a Technical Report that can be matured into a standard and then into a procurement document following international discussion and harmonization of the requirements. As such, we have provided this Technical Report in a format that can readily be transformed to the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standard-compliant format. There are four technical sections or parts to this technical report (namely, Sections 5.1, 5.2, 5.3, and 5.4). If the ILO chooses to standardize this technical report as a biometric profile, the report could be submitted to ISO/IEC JTC 1 SC37, *Biometrics*, and to SC 17, *Identification cards and related devices*.

The authors request that the ILO enhance the verbiage in this document as it sees fit.

Prior to submission, the paragraphs including and preceding this one should be removed from the Forward section of the document. This technical report can be expanded into an application profile in the future to include additional aspects of the SID system, such as issuance, durability, security features, quality control, usage/operational policies, etc. The application profile should also be developed and reviewed by the ILO.

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are

circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75% of the national bodies casting a vote.

This Technical Report was prepared by the International Labour Office (ILO) and can be submitted as a new work item to ISO/IEC JTC 1 SC37, *Biometrics*, and to SC 17, *Identification cards and related devices*.

This Technical Report, ILO SID-0001, consists of the following sections, under the general title *Biometric Profile for Seafarers' Identity Documents*:

- *Part 1: SID fingerprint biometric requirements*
- *Part 2: SID barcode and barcode reader requirements*
- *Part 3: SID identity verification requirements*
- *Part 4: SID database requirements*

## 0 Introduction

### 0.1 Rationale for document development

In the wake of the terrorist attacks of September 11, 2001, the International Labour Organization took steps to revise its 1958 convention on Seafarers' identity documents (also known as "Seafarers' IDs" or "SIDs"), under an accelerated procedure. The new convention, the Seafarers' Identity Documents Convention (Revised), 2003 (Convention No. 185), which was adopted by the International Labour Conference in June 2003, introduced modern security features into the Seafarers' ID to help to resolve the urgent question of seafarers being refused admission into the territory of countries visited by their ships, for the purposes of shore leave and transit and transfer to join or change ships. One of those security features is a fingerprint biometric template, which shall be printed as numbers in a PDF417 bar code "conforming to a standard to be developed" (Convention No. 185, Annex I). In a resolution adopted by the International Labour Conference in June 2003, the ILO Director-General was requested to take urgent measures "for the development by the appropriate institutions of a global interoperable standard" for the biometric template referred to above, particularly in cooperation with the International Civil Aviation Organization (ICAO). At a meeting held at the ILO in September 2003, which was attended by representatives of Governments, Shipowners, and Seafarers, ICAO, and ISO, it became clear that ICAO, which was proceeding with a recommendation for a different biometric solution (see below) as the standard for machine readable passports, was not in a position to take an active part in the development of the template required by the new Seafarers' ID. It was also noted that the urgent time frame required for the entry into operation of Convention No. 185 precluded a resort to the normal procedures for the development of such a template in the framework of the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC).

The International Labour Office has consequently commissioned this Technical Report to reflect the requirements generated by the Seafarers' ID Convention in 2003, which outlined high-level requirements for biometric-based personal identification of the international Seafarer community. The authors submit this Technical Report, ILO SID-0002, in the form of a biometric profile defining the standard for generating and storing minutiae-based fingerprint templates on the PDF417 barcode of the next-generation SID and in the Member's National Electronic Databases (International Labour Convention No. 185, Annex I and Annex II, respectively). This biometric profile is organized in near-ISO-standard-compliant form that can be matured into a standard and then into a procurement document following international discussion and harmonization of the requirements.

### 0.2 Related efforts

Various studies, experiments, pilot programs and products have been developed in recent years in attempts to expedite the inspection process at border management points. Many efforts will incorporate biometric technology into next-generation travel documents and international identification documents. The International Labour Organization drafted and approved Convention No. 185 to define requirements for the next generation Seafarers' IDs, which will incorporate biometric-based personal identification for the seafarer (document holder) and store biometric templates in a barcode printed on the SID.

Prior to 9/11/2001, the biometrics industry had initiated several standards development projects to facilitate the development of interoperable biometrics products and systems, as well as the

interchange of biometrics data objects between products and systems and requirements for insuring the integrity and privacy of biometric data.

- o The American National Standards Institute / InterNational Committee for Information Technology Standards (ANSI/INCITS) standard 358-2002 – Information technology – BioAPI Specification, provides an application programming interface that assures that conforming products and systems can interoperate with each other.
- o ANSI/INCITS 378 – Finger Minutiae-Based Interchange Format, which has been submitted to ISO as a draft standard ISO 19794-2 – Biometric Data Interchange Formats – Part 2: Finger Minutiae Data.
- o The International Civil Aviation Organization (ICAO) standard (document 9303) for Machine Readable Travel Documents (MRTDs) is being commissioned ISO/IEC JTC1 SC17.

NOTE: The latest recommendation of ICAO is to include contactless smart card technology in next generation travel documents and to include one or more biometrics (the facial biometric is required by this standard and either fingerprint or iris recognition systems could also be incorporated). While the ILO Seafarers' ID is an identity document (and not a travel document), the ILO will attempt to comply with the requirements specified in the ICAO proposed standard for next generation MRTD, where possible. It is important to note that the next generation ILO Seafarers' ID will use barcode technology to store biometric data (not the embedded chip recommended by ICAO's MRTD standard). This difference significantly impacts the SID biometric profile as barcode storage capacity is significantly smaller than ICAO-recommended embedded chip storage capacity, but barcode storage is significantly less expensive than embedded chip storage.

Together these standards ANSI/INCITS 358, ANSI/INCITS 378, and the ICAO MRTD, represent the foundation upon which the biometric capabilities of the Seafarers' ID systems will be built. Other standards, either already well established (such as ISO 15438 (PDF417 barcode symbology) and ISO 15416 (PDF417 barcode print quality)) or being developed in parallel with this one (such as the draft standard ISO 19794-4 (Biometric Data Interchange Formats – Part 4: Finger Image Based Interchange Format)) will also be relevant as incorporated below.

Because the next generation ILO Seafarers' ID will use barcode technology to store biometric data and support the ILO's international interoperability requirements of the SID, the SID biometric profile will define the format for PDF417 barcode storage of fingerprint templates. Because fingerprint *image* storage for two fingers will exceed the SID's PDF417 barcode storage capacity, the ILO must specify either *minutiae*-based or *pattern*-based fingerprint biometrics as the basis of procurement. Two Technical Reports have been prepared in support of the ILO's decision. This report, ILO SID-0002, represents the technical requirements for the minutiae-based fingerprint biometric option. The requirements for the pattern-based option are found in ILO SID-0001. The ILO will decide which report (ILO SID-0001 or ILO SID-0002) to prioritize as the basis of next generation SID procurement and to formalize for submission to ISO.

# Biometric Profile for Minutiae-Based Seafarers' Identity Documents

## 1 Scope

This Technical Report, ILO SID-0002, *Biometric Profile for Minutiae-Based Seafarers' Identity Documents*, gives guidelines for incorporation of minutiae-based fingerprint biometric technology into the SID to more tightly bind the identity of seafarers with the Seafarers' ID, in line with the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185), the Functional Brief for the Biometric Template prepared by the Informal Meeting on Biometrics for the SID held on 29-30 September 2003, additional supporting material, the technical consultation meeting in Geneva 5-7 December 2003, and advice of experts in the field.

Biometrics shall be used to increase the strength of the binding between the SID document and the person who holds it.

The report is organized as follows. Conformance requirements for this biometric profile are organized in Section 2. Technical references and definitions that pertain to this document are organized under Sections 3 and 4, respectively. The biometric requirements for the SID are organized under Section 5. There are four major subdivisions under Section 5; namely:

- Section 5.1 *SID minutiae-based fingerprint biometric requirements*, which includes fingerprint enrollment, fingerprint capture, and the SID fingerprint template format to be incorporated into the next generation Seafarers' ID.
- Section 5.2 *SID barcode requirements*, which includes barcode format, printer technology and printing specifications, reader technology, and barcode physical characteristics.
- Section 5.3 *SID identity verification requirements*, which outlines the SID biometric identity verification procedure.
- Section 5.4 *SID database requirements*, which includes barcode database requirements and SID national electronic database requirements.

Annex A details the SID barcode format. Annex B details the SID minutiae-based biometric data format. Annex C includes a copy of draft standard ISO 19794-2 – Biometric Data Interchange Formats – Part 2: Finger Minutiae Data (dated 2003-05-30). And, Annex D includes a copy of draft standard ISO 19794-4 – Biometric Data Interchange Formats – Part 4: Finger image Based Interchange Format (dated 2003-05-29).

Because this fingerprint storage format was developed in accordance with draft ISO standard documents, ***this document will take precedence for the Seafarers' ID*** should evolution of either of these draft standards create any perceived inconsistency.

The following issues are outside of the scope of this Technical Report.

- 1) The overall process of Seafarer identification systems incorporating biometric technologies.
- 2) Criteria for validation of individual Seafarer's identities and of their professional titles.
- 3) Criteria for SID issuance.

- 4) Suitability of other than minutiae-based fingerprint biometric technologies to the Seafarers' ID program.
- 5) Criteria for the "other security features" referred to in the introduction to Annex I of Convention 185.
- 6) Marine environmental issues, including saline crystalline corrosion issues, are out of scope of this biometric profile, but should be addressed in SID procurement specifications.
- 7) Application risk assessments.

## 2 Conformance

A biometric system conforms to this Standard if it correctly performs all the mandatory capabilities defined in Section 5 – SID Biometric Requirements, in Annex A – SID Minutiae-Based Fingerprint Barcode Format, and in Annex B – SID Minutiae-Based Fingerprint Storage Format.

Not all biometric technologies and features are appropriate for the Seafarer ID based on the ILO's requirements and on the maturity of international standards for fingerprint biometric technologies as of the date of this publication. This standard provides the requirements to enable international interoperability of minutiae-based fingerprint biometric components of next-generation Seafarers' IDs; given that minutiae-based fingerprint biometric technology is selected by the ILO for the next generation SID.

## 3 References

This biometric profile is being developed prior to finalization of related draft standards. Any draft standard that is referenced in this section will list the date of publication of the referenced draft. A copy of any referenced draft **conformative standard** (see Section 3.1) will be included as an Annex to this document. Because this fingerprint storage format was developed in accordance with draft ISO standard documents, **this document will take precedence for the Seafarers' ID** should evolution of either of these draft standards create any perceived inconsistency.

### 3.1 Conformative standards

- a) ANSI/INCITS 358-2002 – Information technology – BioAPI Specification
- b) ANSI/NIST-ITL 1-2000 – Data Format for the Interchange of Fingerprint Information – Table 5
- c) ISO/IEC 15416:2000 – Information technology -- Automatic identification and data capture techniques -- Barcode print quality test specification Linear symbols
- d) ISO/IEC 15438 – Information technology -- Automatic identification and data capture techniques -- Barcode symbology specifications PDF417

- e) Draft standard ISO 19794-2 – Biometric Data Interchange Formats – Part 2: Finger Minutiae Data (Draft document dated 2003-05-30)<sup>1</sup>
- f) Draft standard ISO 19794-4 – Biometric Data Interchange Formats – Part 4: Finger Image Based Interchange Format (Draft document dated 2003-05-29)
- g) ISO 14962:1997 -- Space data and information transfer systems -- ASCII encoded English / ANSI INCITS 4-1986 (R2002) Information Systems - Coded Character Sets - 7-Bit American National Standard Code for Information Interchange (7-Bit ASCII)
- h) ISO 3166-1 -- Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes
- i) ISO/IEC 9945-1:2003 -- Information technology -- Portable Operating System Interface (POSIX) -- Part 1: Base Definitions

### 3.2 Informative references

- j) Draft standard ISO/IEC JTC 1/SC 37 N364 – Biometric Profile – Interoperability and Data Interchange – Biometrics-Based Verification and Identification of Employees (Draft document dated 2003-12-01)
- k) ICAO Document 9303 – Machine Readable Travel Document (4<sup>th</sup> Edition, 1999)
- l) ANSI/NIST-ITL-1-2000, Standard Data Format for the Interchange of Fingerprint, Facial, & Scar mark & Tattoo (SMT) Information
- m) ISO/IEC 7810 – Identification cards – Physical characteristics
- n) ISO/IEC 10918 – Information technology – Digital Compression and coding of continuous-tone still images (JPEG) (Parts 1-4)
- o) ISO/IEC 15444 – Information technology – JPEG 2000 Image Coding System (Parts 1-10)

### 3.3 Additional standards and documentation to be developed

- p) Biometric Profile for Pattern-Based Seafarers' Identity Documents
- q) SID Application Profile Standard
- r) SID Performance and Interoperability Testing and Reporting Standard
- s) An adequate and user-friendly guidance document for taking fingerprints to assist the enrolment personnel to produce reproducible and reliable results.

---

<sup>1</sup> ANSI/INCITS has just announced formalization of this standard under the title ANSI/INCITS 378 – Finger Minutiae-Based Interchange Format.

## 4 Terms and definitions

The authors have attempted to ensure that the terms, definitions, symbols, and abbreviated terms of this Technical Report conform to the emerging Standard for Biometric Vocabulary Harmonization, being developed by Working Group 1 of ISO/IEC JTC 1 SC 37. Specific relevant terms are defined below for the reader's convenience.

### 4.1 Terms and definitions

#### 4.1.1 Application profile

Conforming subsets or combinations of base standards used to provide specific functions. Application profiles identify the use of particular options in base standards, and provide a basis between applications and interoperability of systems.

#### 4.1.2 ASCII

Using the ISO 14962:1997 / ANSI-X3.4-1986(R1997) character set.

#### 4.1.3 Biometric

Pertaining to the field of biometrics, used as an adjective.

NOTE: "biometric" should no longer be used as a noun.

#### 4.1.4 Biometric authentication/biometrically authenticate

The use of biometric verification or identification to validate the authenticity of someone.

#### 4.1.5 Biometric data block (BDB)

A block of data with a defined format that contains one or more biometric samples or biometric templates.

#### 4.1.6 Biometric identification/biometrically identify

A one-to-many or one-to-few process of comparing an individual's biometric sample against a database of biometric reference data to either (1) discern the identity of an enrolled individual using only the presented biometric data (Positive identification); or (2) ensure the absence of an individual's biometric reference data with respect to a database (Negative identification).

#### 4.1.7 Biometric information record (BIR)

A data structure containing a BDB, information identifying the BDB format, and possibly further information such as whether the BDB is digitally signed or encrypted.

#### 4.1.8 Biometric interchange data record (BIDR)

A data structure, corresponding to one person, that contains a BIR (see 4.1.7) plus other information specific to Seafarer ID systems, applications, or functions.

#### 4.1.9 Biometric sample

Information obtained from a biometric device, either directly or after further processing.

#### **4.1.10 Biometric verification/biometrically verify**

A one-to-one comparison of an individual's biometric sample with the individual's biometric reference template in order to validate an explicit positive claim on identity. (May also include one-to-few comparisons of multiple reference templates for the same individual).

#### **4.1.11 Biometrically enroll**

The process of collecting one or more biometric samples from a subject and the subsequent preparation and storage of one or more processed biometric samples and associated data representing that subject's identity.

#### **4.1.12 Country Code**

The numeric three-digit country code defined in ISO 3166-1.

#### **4.1.13 Global interoperability of SID biometric data**

Global acceptance of the SID fingerprint biometric data block stored in the 2-D barcode printed on the SID for Seafarer verification.

#### **4.1.14 Null-terminated string**

A string of data that terminates with a zero byte (0x00).

#### **4.1.15 Real-time**

Of or pertaining to a mode of computer operation in which the computer collects data, computes with it, and uses the results to control a process as it happens.

#### **4.1.16 Seconds since the epoch (SSE)**

Seconds since the epoch, in a 32-bit unsigned integer, of the day specified. Recommend using the first second of that day, but any second of a specified day is allowed. See ISO/IEC 9945-1:2003 4.14.

#### **4.1.17 Shall**

In accordance with legislative practice, the term "shall" indicates a mandatory practice.

#### **4.1.18 Should**

In accordance with legislative practice, the term "should" indicates a recommended practice that is not mandatory.

#### **4.1.19 SID data integrity**

The property of physically stored data, both on a Seafarer's ID and in a central database(s), that the data cannot be altered without such alteration being detected and tracked.

#### **4.1.20 SID data privacy**

The property of physically stored data, both on a Seafarer's ID and in a central database(s), that the data cannot be accessed or processed except by people or applications that have the specific rights and technological capability to do so.

## 5 SID biometric requirements

### 5.1 SID minutiae-based fingerprint biometric requirements

Two minutiae-based fingerprint biometric templates of the Seafarer to whom the document has been issued shall be printed as numbers in a barcode conforming to the standard outlined in this document. The ILO Convention No. 185 has a set of preconditions that must be met by the resultant system, which are highlighted below with the compliance strategy assumed by the authors of this biometric profile.

- “The fingerprint can be captured without any invasion of privacy of the persons concerned, discomfort to them, risk to their health or offense against their dignity;” (International Labour Convention No. 185, Article 3, paragraph 8 (a))

*This requirement is addressed with the assumption that Seafarers will not perceive fingerprint capture and verification to be an invasion of their privacy or an offense against their dignity. It also assumes that the implementation of biometric systems and barcode readers will be installed ergonomically such that no discomfort to the Seafarer is imposed. It furthermore assumes that risk to the Seafarers' health is assessed upon system implementation and checkout; and that the systems will be routinely sanitized to prevent the spread of germs via contact with system components, such that there is no greater health risk in using the fingerprint capture device than there would be in using a door knob, for example.*

- “The biometric [data] shall itself be visible on the document and it shall not be possible to reconstitute it from the template or other representation;” (International Labour Convention No. 185, Article 3, paragraph 8 (b))

*This requirement presumes that it is sufficiently difficult to reconstitute an actual fingerprint (understood as “fingerprint image”) from the biometric data that will be stored in the barcode. It also presumes that the biometric data shall be considered visible when the barcode in which fingerprint biometric data is stored is printed on the next-generation SID.*

- “The equipment needed for the provision and verification of the biometric [sample] is user-friendly and is generally accessible to governments at low cost;” (International Labour Convention No. 185, Article 3, paragraph 8 (c))

*This presumes that the “user-friendly” requirement can and will be satisfied via biometric system ergonomics by implementers and system users. It also assumes that the ILO's selection of barcode storage for the fingerprint data satisfies the requirement for “generally accessible to governments at low cost”.*

- “The equipment [used] for the verification of the biometric [sample] can be conveniently and reliably operated in ports and in other places, including on board ship, where verification of identity is normally carried out by the competent authorities;” (International Labour Convention No. 185, Article 3, paragraph 8 (d))

*This presumes that the biometric and card reading systems will be able to be reliably used onboard ships, in ports, and other places, such that the systems are not considered unusually susceptible to the corrosive saline atmospheric environments found in these areas.*

- "The system in which the biometric [authentication] is to be used (including the equipment, technologies and procedures for use) provides results that are uniform and reliable for the authentication of identity." (International Labour Convention No. 185, Article 3, paragraph 8 (e))

*This presumes that "uniform" implies conforming to this technical report to ensure interoperability. It also presumes that commercial biometric systems satisfy reliable "authentication of identity" (understood "verification of identity") for the Seafarer population that will be utilizing these systems.*

### 5.1.1 Enrollment

A fingerprint should be captured from the index finger of each hand.<sup>2</sup> If the index fingerprint is missing or damaged to the extent that a reliable fingerprint either cannot be created or cannot be enrolled due to poor quality, a fingerprint from another finger or thumb will be captured such that operational consistency, operational efficiency, and Seafarer convenience are maximized. The standard presentation order of fingers for enrollment is given below:

- right index finger,
- left index finger,
- right thumb,
- left thumb,
- right middle finger,
- left middle finger,
- right ring finger,
- left ring finger,
- right little finger,
- left little finger.

The specific fingers enrolled shall be recorded in the header of the template. (see Appendix A and ANSI/INCITS 358-2002 – Information technology – BioAPI Specification).

The system should either automatically incorporate a quality measure or provide a quality measure to enrollment personnel along with a minimum acceptable quality measure to ensure that good quality templates are generated (collected, captured). The best possible quality fingerprint templates should be enrolled to achieve reliable verification results.

User-friendly documentation shall be provided that instructs personnel how to perform the enrollment process and how to ensure that good quality fingerprint templates are enrolled.

---

<sup>2</sup>Fingerprints from two fingers are acquired to improve the reliability and robustness of the system. The index finger is chosen for the primary fingerprint because in most cases, the index finger is most easily placed on the fingerprint capture device, thus providing maximum convenience to the seafarer (Convention, Article 3, paragraph 8, Precondition 1)

### 5.1.2 Fingerprint capture

During both enrollment and verification, the fingerprint capture device shall acquire minutiae-based fingerprint biometric templates that conform to Table 1 in Annex A of the draft standard ISO/IEC 19794-4<sup>3</sup> (see Annex D of this document for the entire draft standard) with a minimum fingerprint data capture quality level of 3<sup>4</sup> as summarized below.

- Scan resolution: 197 pixels/cm (500 pixels/inch)
- Pixel scale depth: 8 bits
- Dynamic range (gray levels): 220
- Certification: EFTS/F

The fingerprint capture device shall produce a 12.7 by 12.7 mm (0.5 by 0.5 inch) image of the fingerprint or the image shall be centered, preferably on the core of the fingerprint, then cropped or padded as needed to achieve this image size.

When the fingerprint image is transmitted to the template extraction algorithm, such as from the capture device to a computer, the data shall either be uncompressed or use the "lossless" WSQ compression dictated by draft standard ISO/IEC 19794-4.

### 5.1.3 Fingerprint template

The algorithm shall extract a fingerprint template from the acquired fingerprint image in conformance with ISO/IEC 19794-2, Biometric Data Interchange Formats – Part 2: Finger Minutiae Data. The fingerprint templates will be stored in the Member State's national electronic database (Convention database) and in the PDF417 2-D barcode on the SID during the enrollment process and used for matching during the verification process.

A fingerprint template is stored instead of the fingerprint image for two reasons:

1. To respect and protect the privacy of the seafarer. Article 3, paragraph 8, Precondition 3 requires that it shall not be possible to reconstitute the fingerprint image from the stored fingerprint data. If the ILO chose to store unencrypted fingerprint images, then it would be possible to reconstitute the Seafarers' fingerprint images. As a result, the ILO has determined that fingerprint templates shall be stored on the SID barcode to satisfy this requirement.
2. The memory required to store the fingerprint image, whether encrypted or unencrypted, is beyond the storage capacity of a PDF417 2-D barcode.

The minutiae-based fingerprint template is selected over the pattern-based template for two reasons:

1. Many SID issuance organizations already utilize minutiae-based fingerprint technology for other purposes. The ILO hopes to leverage these systems if possible to address SID requirements.
2. The international law enforcement community predominantly employs minutiae-based template technology, and the law enforcement community will play a role in identity proofing prior to SID issuance.

---

<sup>3</sup> This Working Draft standard is currently a proposed standard that is under revision by ISO/IEC JTC 1 SC37 Working Group 3. We do expect the quality level 3 parameters to remain the same as the draft standard migrates to an approved standard. Nevertheless, the parameters specified in this document will take precedence for the SID.

<sup>4</sup> Fingerprint data capture quality level 3 is acceptable for images to be used to generate minutiae-based fingerprint templates. Note that the fingerprint data capture quality is separate and distinct from the print image quality of the SID barcode.

Fingerprints may contain a variable number of minutiae points. The number of minutiae points will therefore range from only a few to more than can be stored without exceeding the fixed storage range of the SID PDF417 2-D barcode. A number field is therefore included in the template specifying the number of minutiae points recorded in the stored template. Only the most centrally located points will be included in the recorded template if the total number exceeds the capacity of storage.

In accordance with proposed standard ISO/IEC 19794-2, the ILO SID minutiae-based biometric template has been specified in Annexes A, B, and C. The biometric template structure is summarized below:

- BioAPI -compliant header - 16 bytes
- Record header - 26 bytes
- Two finger minutiae templates – up to 776 bytes
- Each finger minutiae template shall have up to 64<sup>5</sup> minutiae stored in terms of x position, y position, ridge angle, and type.
- Total template size for two fingerprints - 818 bytes

## 5.2 SID barcode requirements

### 5.2.1 Barcode format

The SID barcode shall be formatted in accordance with Annex A. The minutiae-based fingerprint SID barcode will contain up to 938 bytes of data, and 64 data symbols for error correction level 5. The barcode shall contain the biometric template information and information that shall be printed on the face of the SID; specifically: the issuing authority, the full name of the Seafarer, the unique document number, and the date of expiry of the document. The Seafarers' biometric templates for two fingerprints shall be formatted in accordance with Annex B, which defines the 818 byte biometric data block referenced in Annex A.

PDF417 2-D barcode technology shall be implemented for the following reasons:

- PDF417 symbols meet the data storage capacity requirements of this application.
- PDF417 symbols can be read with a 2-D scanner or with standard CCD or laser scanners and special decoding software. Wand scanners, however, will not read PDF417 symbols. This wide range of affordable, commercial barcode reader technology products will facilitate biometric verification of the Seafarer community.

Dimensions and placement of the barcode shall conform to International Civil Aviation Organization (ICAO) specifications as contained in Document 9303 Part 1 (5th edition, 2003) and Document 9303 Part 3 (2nd edition, 2002) as outlined below for reader convenience:

- For SID booklets the maximum barcode size is 18.35mm x 86.0mm including quiet zones as specified in ICAO Document 9303 Part 1 -- Machine Readable Passports -- Annex A

<sup>5</sup> Derivation of the number of minutiae per finger for SID barcode fixed format storage follows. There are 25 data symbol columns, which give 25 data symbols in a row. There are 34 rows. There are 25 x 34 = 850 data symbols total. Level 5 error correction uses 64 data symbols, so there are 850-64 = 786 data symbols for SID ILO use. There are 1.2 bytes/data symbol. There are 786 x 1.2 = 943 bytes of storage. 943 – 120 metadata bytes (see Annex A) = 823 bytes of biometric storage. The BioAPI minutiae header is 42 bytes, so 823 – 42 = 781 bytes remain for two fingerprint templates. Each minutiae template requires 4 bytes of additional header information, so 8 bytes are required for two fingerprint templates. 781 – 8 = 773 bytes of storage for minutiae templates. Each minutiae requires 6 bytes of storage. So, 773 / 6 = 128 minutiae total. If the template size is fixed and there are 2 fingers, then the number of minutiae per finger is given by the result 128 / 2 = 64 minutiae per finger.

(normative) Use of Optional Barcode(s) on Machine-Readable Passport (MRP) Data Page.

- For SID cards the maximum barcode size is 27.8mm x 85.6mm including quiet zones as specified in ICAO Document 9303 Part 3 -- Size 1 and Size 2 Machine Readable Official Travel Documents -- Appendix 2.

In addition, the SID barcode shall conform to the following:

- X-dimension: minimum width of symbol module is 0.17 mm (larger to fill card area, if possible, up to a maximum size of 0.25 mm).
- Y-dimension: minimum height of row is 0.51 mm (3 times X-dimension, larger to fill card area, if possible, up to a maximum size of 0.75 mm).
- Error correction level 5 as recommended in ISO 15438 Annex E.
- Number of data symbol columns = 25.
- Number of rows as necessary to contain the data (34 rows<sup>6</sup>).

### 5.2.2 Printer technology and printing specifications

The SID PDF417 barcode shall be printed in accordance with ISO 15438. PDF417 2-D barcode symbols can be printed with most professional-grade thermal transfer, laser, and ink jet label printers. Next-generation SID barcode Print Quality shall conform to ISO/IEC 15416:2000(E) - Barcode print quality test specification - Linear symbols, as 3.0/05/660. The designation 3.0/05/660 refers to an overall symbol grade of 3.0, obtained using a 0.125 mm aperture, at a wavelength of 660 nm.

SID barcodes shall be printed such that the resultant document is durable enough to withstand use as an identification document for Seafarers.

### 5.2.3 Reader technology

Next-generation SID PDF417 symbols will be read with a 2-D scanner, or with standard CCD or laser scanners and special decoding software that read barcodes printed in compliance with Sections 5.2.1 and 5.2.2 above. Wand scanners, however, will not read PDF417 symbols.

### 5.2.4 Barcode physical characteristics

The "biometric template based on a fingerprint printed as numbers in a bar code" (International Labour Convention No. 185, Annex I, paragraph 3(k)) "shall be protected by a laminate or overlay, or by applying an imaging technology and substrate material that provides an equivalent resistance to substitution of the portrait and other biographical data. (International Labour Convention No. 185, Annex I). This protection will also improve the durability of the barcode.

The "biometric shall itself be visible on the document" (International Labour Convention No. 185, Article 3, paragraph 8(b)). This requirement is interpreted to mean that the biometric data shall be considered visible when the barcode in which fingerprint biometric data is stored is printed on the next-generation SID. Therefore, the barcode shall be visible when printed on the SID.

<sup>6</sup> The number of rows in the SID fixed format barcode is 34. This represents the maximum size of a fixed barcode suitable for printing on both card-type and booklet-type SIDs, which assumes that minutiae templates will be padded with zeroes if less than 64 minutiae per fingerprint template.

## 5.3 SID identity verification requirements

### 5.3.1 Verification Procedure

A barcode reader shall scan the barcode on the SID and read the header and template information. The header shall specify which fingers' prints are stored in the barcode.

The system shall be configurable in that it shall prompt the Seafarer to present either one of the fingers previously enrolled on a fingerprint capture device or both those fingers (sequentially), for the purpose of capture and comparison with the data stored in the barcode.

If the system is configured such that only one live scan fingerprint must match with one of the templates stored on the barcode during enrollment for Seafarer authentication, the system shall prompt the Seafarer for the first finger template read from the barcode (see Section 5.1.1). If the Seafarer's finger corresponding to the first finger enrolled is unavailable, damaged, does not acquire, or does not achieve a matching score above the threshold value after three attempts, the system shall prompt the Seafarer to place the second finger enrolled on the biometric capture device. If one live scan finger matches the corresponding templates stored on the barcode, the Seafarer shall be successfully verified. If no live scan fingers match either of the corresponding templates stored on the barcode, the system shall return a failure to verify indication.

If the system is configured such that live scan fingerprints must match both of the templates stored in the barcode during enrollment for Seafarer authentication, the system shall prompt the Seafarer to place finger corresponding to the first finger template read from the barcode (see Section 5.1.1) on the biometric capture device. If the Seafarer's first finger successfully matches the template stored on the barcode, the system shall prompt the Seafarer to place the finger corresponding to the second finger template read from the barcode on the biometric capture device. If both templates stored on the barcode match the corresponding live scan fingers, the Seafarer shall be successfully verified. If either of the enrolled fingers are unavailable, damaged, do not acquire, or do not achieve a matching score above the threshold value after three attempts, the system shall return a failure to verify indication.

The biometric fingerprint system shall:

- Retrieve the template from the SID PDF417 2-D barcode,
- Prompt the Seafarer to place the appropriate finger on the image capture sensor.
- Generate a template from the live sample capture (see Section 5.1.3).
- Compare the acquired fingerprint template with the fingerprint template that is stored in the 2-D barcode.
- Provide a match indication (identity verified) if the matching score is above the matching threshold and provide a non-match indication (identity not verified) if the matching score is below the matching threshold.

The fingerprint biometric system should:

- Have the matching threshold set to a level that will be commensurate with a false finger match of less than 1% and a false reject rate of less than 1%.
- Have sensitivity and quality measures that are commensurate with quality metrics for enrollment.
- Optionally provide a measure indicating the quality of the acquired fingerprint template.

### 5.3.2 Documentation

User-friendly documentation shall be provided that instructs personnel how to perform the verification process.

## 5.4 SID database requirements

### 5.4.1 Barcode database

"Seafarers shall have convenient access to machines enabling them to inspect any data concerning them that is not eye-readable. Such access shall be provided by or on behalf of the issuing authority." (International Labour Convention No. 185, Article 3, paragraph 9) "Biometric template shall be based on a fingerprint printed as numbers in a bar code conforming to a standard" [this standard] (International Labour Convention No. 185, Annex I).

*The issuing authority shall provide Seafarers access to machines enabling them to inspect the data stored in the SID PDF417 2-D barcode. This data will be displayed in a series of binary numbers (1's and 0's) conforming to the format defined in Annex A of this technical report.*

### 5.4.2 SID national electronic database

The ILO Convention No. 185 has a set of requirements that must be met and a set of requirements that should be met by each Member with regard to the SID national electronic database that will impact the biometric system implementation and use. These requirements are highlighted below with the compliance strategy assumed by the authors of this biometric profile.

- "The details to be provided for each record in the electronic database to be maintained by each Member in accordance with Article 4, paragraphs 1, 2, 6 and 7 of this [International Labour Conference] Convention [185] shall be restricted to:
  1. Issuing authority named on the identity document.
  2. Full name of seafarer as written on the identity document.
  3. Unique document number of the identity document.
  4. Date of expiry or suspension or withdrawal of the identity document.
  5. Biometric template appearing on the identity document.
  6. Photograph.
  7. Details of all inquiries made concerning the seafarers' identity document." (International Labour Convention No. 185, Annex II).

*The national electronic database shall contain records of the seven items listed above for each Seafarer that is issued a SID.*

- "For the purposes of this Convention, appropriate restrictions shall be established to ensure that no data – in particular, photographs – are exchanged, unless a mechanism is in place to ensure that applicable data protection and privacy standards are adhered to." (International Labour Convention No. 185, Article 4, paragraph 6).

*Database access control mechanisms shall be implemented to protect Seafarer information from unauthorized persons and unintended purposes.*

- "The particulars of each item contained in [International Labour Convention No. 185] Annex II are [shall be] entered in the database simultaneously with issuance of the SID". (International Labour Convention No. 185, Annex III, Part A, paragraph 3 (b)(i)).

*Member national electronic databases shall be updated with each SID issued in a timely manner.*

- "Each Member shall ensure that a record of each seafarers' identity document issued, suspended or withdrawn by, it is stored in an electronic database. The necessary measures shall be taken to secure the database from interference or unauthorized access." (International Labour Convention No. 185, Article 4, paragraph 1). "The seafarers' identity document shall be promptly withdrawn by the issuing State if it is ascertained that the seafarer no longer meets the conditions for its issue under this Convention". (International Labour Convention No. 185, Article 7, paragraph 2). "The issuing authority should draw up adequate procedures for protecting the database, including the restriction to specially authorized officials of permission to access or make changes to an entry in the database once the entry has been confirmed by the official making it." (International Labour Convention No. 185, Annex III, Part B. paragraph 4.2.2).

*Member national electronic databases shall implement an audit function that will log transactions including SID issuance, SID suspension, or SID withdrawal / cancellation. Database access control mechanisms shall be implemented to protect Seafarer information from unauthorized persons and unintended purposes. Specially authorized officials within each Member's organization should have limited ability to make changes to the audit log; documentation of any such changes should be maintained by the Member.*

- "Prompt action is [shall be] taken to update the database when an issued SID is suspended or withdrawn". (International Labour Convention No. 185, Annex III, Part A, paragraph 3 (c)).

*Member national electronic databases shall be updated in a timely manner when SIDs are suspended or withdrawn.*

- "An extension and/or renewal system has been [shall be] established to provide for circumstances where a seafarer is in need of extension or renewal of his or her SID and in circumstances where the SID is lost" (International Labour Convention No. 185, Annex III, Part A, paragraph 3 (d)). ". "The applicant should not be issued a SID for so long as he or she possesses another SID." (International Labour Convention No. 185, Annex III, Part B. paragraph 3.9).

*Members shall implement an extension and/or renewal system to provide for circumstances where a seafarer is in need of extension or renewal of his or her SID and in circumstances where the SID is lost. SID extension and/or renewal shall create a transaction in the national electronic database a timely manner. In the event that a SID is rejected due to expiration, the national electronic database shall be checked to see if the SID has been extended or renewed. Seafarers' should only possess one SID at a time. A reissued SID should invalidate any SID previously issued to the Seafarer. The biometric system shall support SID reenrollment or reissuance.*

- "An early renewal system should apply in circumstances where a seafarer is aware in advance that the period of service is such that he or she will be unable to make his or her application at the date of expiry or renewal" (International Labour Convention No. 185, Annex III, Part B. paragraph 3.9.1). ". "The applicant should not be issued a SID for so long as he or she possesses another SID." (International Labour Convention No. 185, Annex III, Part B. paragraph 3.9).

*Members shall implement an extension and/or renewal system to provide for circumstances where a seafarer is in need of extension or renewal of his or her SID. The Seafarer shall be able to instigate an extension and/or renewal at his or her convenience given that he or she will not be able to make his or her scheduled application for renewal. SID extension and/or renewal shall create a transaction in the*

*national electronic database in a timely manner. In the event that a SID is rejected due to expiration, the national electronic database shall be checked to see if the SID has been extended or renewed. Seafarers' should only possess one SID at a time. A reissued SID should invalidate any SID previously issued to the Seafarer. The biometric system shall support SID reenrollment or reissuance.*

- "A replacement system should apply in circumstances where a SID is lost. A suitable temporary document can be issued. (International Labour Convention No. 185, Annex III, Part B. paragraph 3.9.3). "The applicant should not be issued a SID for so long as he or she possesses another SID." (International Labour Convention No. 185, Annex III, Part B. paragraph 3.9).

*Members shall implement a replacement system to provide for circumstances where a seafarer loses his or her SID. SID replacement shall create a transaction in the national electronic database in real time. Seafarers' should only possess one SID at a time. A reissued SID should invalidate any SID previously issued to the Seafarer. The biometric system shall support SID reenrollment or reissuance. The Seafarer shall be able to instigate a replacement SID for any temporary document at his or her convenience. The temporary document will be surrendered. The national electronic database shall be updated to reflect the changes in a timely manner.*

- "The issuing authority should draw up adequate procedures for protecting the database, including a requirement for the regular creation of back-up copies of the database, to be stored on media held in a safe location away from the premises of the issuing authority." (International Labour Convention No. 185, Annex III, Part B. paragraph 4.2.2).

*Each Member's issuing authority should regularly create back-up copies of the national electronic database which should be stored on media held in a safe location away from the premises of the issuing authority.*

- "Records of problems with respect to the reliability or security of the electronic database, including inquiries made to the database" should be maintained by the issuing authority within each Member. (International Labour Convention No. 185, Annex III, Part B. paragraph 5.6.5).

*Member national electronic databases shall implement an audit function that will log problems impacting the reliability or security of the electronic database (including inquiries made to the database.*

## Annex A: SID Minutiae-Based Fingerprint Barcode Format

The SID PDF417 2-D barcode shall have 25 data symbol columns and a maximum of 34 rows, utilizing error correction level five. The data shall be recorded using byte-mode. There shall be a total of 938 bytes of data in the SID minutiae-based fingerprint barcode format, described below. The Seafarers' fingerprint biometric data shall be recorded using the format specified in Annex B followed immediately thereafter by a set of metadata that is both printed on the surface of the SID in text and in the barcode to support Seafarer authentication.

<b>Minutiae-Based Fingerprint SID Barcode Format</b>			
<i>Field</i>	<i>Size</i>	<i>Format</i>	<i>Comments</i>
Fingerprint Data	818Bytes	See Annex B	Data for two fingerprint templates of up to 64 minutiae each in BioAPI compliant format. If less than 64 minutiae per finger, pad with zeroes.
Issuing Authority	2 Bytes	ISO Code	The country code of the issuing authority stored as an unsigned integer in two bytes. (See Note 1)
Document Number	9 Bytes	ASCII	An ASCII string of up to nine characters stored in nine bytes. The string consisting of the issuing authority and the document number shall be unique. (See Note 1)
Personal Identification Number	14 Bytes	ASCII – Optional	An optional null terminated ASCII string of up to 14 characters stored in 14 bytes. A string of 14 null bytes may be stored instead.
Expiry Date	4 Bytes	SSE	Stored in Seconds Since Epoch (SSE) format.
Primary Identifier	20 Bytes	ASCII	A null-terminated ASCII string in 20 bytes using up to 20 characters.
Secondary Identifier	20 Bytes	ASCII	A null-terminated ASCII string in 20 bytes using up to 20 characters.
Nationality	2 Bytes	ISO Code	An unsigned integer in two bytes.
Place of Birth	20 Bytes	ASCII	A null-terminated ASCII string in 20 bytes using up to 20 characters.
Date of Birth	4 Bytes	SSE	Stored in SSE format.
Gender	1 Byte	ASCII	'm' (0x6D) or 'f' (0x66) or 'x' (0x78).
Date of Issue	4 bytes	SSE	Stored in SSE format.
Place of Issue	20 Bytes	ASCII	A null-terminated ASCII string in 20 bytes
<b>Note 1: The Issuing Authority plus the Document Number comprise the Unique Document Identifier</b>			

## Annex B: SID Minutiae-Based Fingerprint Barcode Storage Format

The SID barcode will be generated in a fixed format to support international interoperability. Data for two minutiae-based fingerprints will be stored in a fixed-size PDF417 barcode structure in accordance with ISO 15438 that uses the draft ISO/IEC minutiae-based fingerprint interchange format (19794-2) to encode two fingerprints with 64 minutiae each (in the event that a fingerprint has less than 64 minutiae the fixed size template for the SID shall be padded with zeros), and wrapped inside a BioAPI template as outlined in the Table below.

Because this fingerprint storage format was developed in accordance with draft ISO standard documents, this document will take precedence for the Seafarers' ID should evolution of either of these draft standards create any perceived inconsistency. Copies of the two draft conformance standards; namely, draft standard ISO 19794-2<sup>7</sup> – Biometric Data Interchange Formats – Part 2: Finger Minutiae Data (Draft document dated 2003-05-30) and draft standard ISO 19794-4 – Biometric Data Interchange Formats – Part 4: Finger Image Based Interchange Format (Draft document dated 2003-05-29), are provided in Annex C and Annex D, respectively.

Many values will be the same for every template, as indicated below. Refer to Annex C for encoding details. In no event shall an optional field be skipped. All fields marked as 'Fixed' shall not contain values other than those present. Some fields are "RIU" -- Reserved for Implementers Use. To assist in implementation, many field names from the BioAPI standard are used here.

<b>SID Minutiae-Based Fingerprint Barcode Storage Format</b>			
<i>Field</i>	<i>Size</i>	<i>Value</i>	<i>Comment</i>
<b>BioAPI_BIR (Biometric Identification Record)</b>			
<b>BioAPI_BIR_HEADER</b>			
Length in Bytes	4 Bytes	up to 0x00000362	up to 854 Bytes (length of record + 16)
BioAPI_BIR_VERSION	1 Byte	0x01	Fixed
BioAPI_BIR_DATA_TYPE	1 Byte	0x04	Fixed -- "Processed"
BioAPI_BIR_BIOMETRIC_DATA_FORMAT	4 Bytes	0x01010301	Fixed -- 0x0101 == JTC 1 SC 37 format owner 0x0301 == Fingerprint Minutiae-Based template with no extended data
BioAPI_Quality	1 Byte		signed integer
BioAPI_BIR_PURPOSE	1 Byte	0x02	Fixed -- BioAPI_PURPOSE_IDENTIFY
Bio_API_BIR_AUTH_FACTORS	4 Bytes	0x00000008	Fixed -- BioAPI_FACTOR_FINGERPRINT

<sup>7</sup> ANSI/INCITS has just announced formalization of this standard under the title ANSI/INCITS 378 – Finger Minutiae-Based Interchange Format.

<b>SID Minutiae-Based Fingerprint Barcode Storage Format</b>			
<i>Field</i>	<i>Size</i>	<i>Value</i>	<i>Comment</i>
<b>BioAPI "Opaque Biometric Data"</b>			
Format Identifier	4 Bytes	0x464D5200	Fixed -- "FMR" 0x00
Version Number	4 Bytes	0x32484900	Fixed -- "20" 0x00
Length of Record	2 Bytes	up to 0x0352	up to 838 Bytes (total # of minutiae * 6 + 34)
CBEFF Product Identifier	4 Bytes		RIU
Capture Equipment Compliance	4 bits		RIU
Capture Equipment ID	12 bits		RIU
X (horizontal) Image Size	2 Bytes		Pixels per centimeter
Y (vertical) Image Size	2 Bytes		Pixels per centimeter
X (horizontal) resolution – Minutiae	2 Bytes		Pixels per centimeter
Y (vertical) resolution – Minutiae	2 Bytes		Pixels per centimeter
Number of fingers	1 Byte	0x01	Fixed -- Two fingers
Reserved Byte	1 Byte	0x00	Fixed -- For future use
<b>1st Fingerprint</b>			
Finger Location	1 Byte	0x01 - 0x0A	0x02 == Right Index Finger 0x07 == Left Index Finger 0x01 == Right Thumb 0x06 == Left Thumb 0x03 == Right Middle Finger 0x08 == Left Middle Finger 0x04 == Right Ring Finger 0x09 == Left Ring Finger 0x05 == Right Little Finger 0x0A == Left Little Finger (From ANSI/NIST-ITL 1-2000* Table 5)
View Number	4 bits	0x0	
Impression Type	4 bits	0x0 or 0x8	0x00 == Live-scan plain 0x08 == Swipe 0x09 == Reserved for future use
Finger Quality	1 Byte	0x00-0x64	0-100
Number of Minutiae	1 Byte	up to 0x43	up to 64 Minutiae
Finger Minutiae Data	384 Bytes		See Annex C. If the number of minutiae is less than 64, pad with zeroes.

<b>SID Minutiae-Based Fingerprint Barcode Storage Format</b>			
<i>Field</i>	<i>Size</i>	<i>Value</i>	<i>Comment</i>
<b>2nd Fingerprint</b>			
Finger Location	1 Byte	0x01 - 0x0A	0x02 == Right Index Finger 0x07 == Left Index Finger 0x01 == Right Thumb 0x06 == Left Thumb 0x03 == Right Middle Finger 0x08 == Left Middle Finger 0x04 == Right Ring Finger 0x09 == Left Ring Finger 0x05 == Right Little Finger 0x0A == Left Little Finger (From ANSI/NIST-ITL 1-2000" Table 5)
View Number	4 bits	0x0	
Impression Type	4 bits	0x0 or 0x8	0x00 == Live-scan plain 0x08 == Swipe 0x09 == Reserved for future use
Finger Quality	1 Byte	0x00-0x64	0-100
Number of Minutiae	1 Byte	up to 0x43	up to 64 Minutiae
Finger Minutiae Data	384 Bytes		See Annex C. If the number of minutiae is less than 64, pad with zeroes.

## Annex C - draft standard ISO 19794-2

## Annex D - draft standard ISO 19794-4

(b)(6)

From: (b)(6)  
Sent: Thursday, May 06, 2004 4:45 PM  
To: (b)(6)  
Cc: Dale, Kevin CAPT  
Subject: FW: Biometrics survey



DHS FingerprintsLicense FingerprintsCertific FingerprintsMarineS ILO SID-0002 r0  
tricSurveyNMCMay2 46CFR.pdf ation46CFR... afetyManual... Minutiae-Based...

> Ms. Stephen,

>  
> Please find attached the completed biometric survey submitted on behalf of  
> the Coast Guard, G-MPS.

>  
> In addition, I've attached the agreed upon biometric standard for the  
> International Seafarers' Identity Document adopted by the International  
> Labor Organization in ILO Convention 185 and supported by the  
> International Maritime Organization as part of a new comprehensive  
> international maritime security system. We expect that the ILO 185  
> standards will be widely adopted by the international seafarer community  
> within the next 1-3 years. It is not currently a biometric standard  
> employed by the USCG, so it should not be reported in the survey, but I  
> provide it for your information.

> Please don't hesitate to contact me if you require further information.

> Respectfully,

> (b)(6)  
> U.S. Coast Guard (G-MPS-2)  
> Port Security Directorate  
> Phone: (b)(2), (b)(6)  
> Fax: (b)(6)

> <<DHS BiometricSurveyNMCMay2004.doc>> <<FingerprintsLicense46CFR.pdf>>  
> <<FingerprintsCertification46CFR.pdf>>  
> <<FingerprintsMarineSafetyManual.pdf>>  
>  
> <<ILO SID-0002 r0 Minutiae-Based Biometric Profile\_20040117.doc>>

## **Attachment 7 Biometrics Survey: CBP FAST**

**Free and Secure Trade Program (FAST).** The FAST driver identification RFID card issued to the driver as a result of a successful background check (10 print fingerprint check) provides Customs and Border Protection Officers at land border cargo crossings with a highly reliable form of identification of a low risk driver.

The unique RFID identification number contained on a computer chip embedded in the card is linked to a specific driver record in the FAST national driver registration database. The front of the card contains the driver picture, which is captured at the time the card is issued, along with the driver's name, date of birth, and a barcode representation of RFID identification number.

Upon arrival at a FAST equipped cargo lane the driver's RFID identification number is automatically detected and forwarded to the national data center where it is match against the driver registration database. The result of the match causes the driver picture, name and date of birth to be made available to the primary inspector. If no RFID scanner or antenna is available, Officers can obtain the database record by scanning the barcode or entering name and date of birth. If the database information, including driver photo do not match the card, it is highly likely that the card is not valid.

### **What is the type of biometrics technology used?**

Integrated live scan fingerprinting system that captures prints and transmits fingerprints without the use of ink are used to determine if a driver has a criminal history. Digital photographs are also used on the FAST driver's card as a means of identification.

### **How much did it cost your agency to implement the use of biometrics for the program/initiative and what is the FY04 projected cost for using the technology?**

398,400 for hardware. FBI costs \$16 per applicant x 19,506 applicants = \$19,522

$\$398,400 + \$19,522 = \$417,922$  Additional costs for FY 04 will depend on the number of driver cards issued.

### **Is the use of biometrics for this program or initiative mandated by statute or rule?**

The FAST program was announced with a Federal Register Notice 12/17/2002.

### **How is the biometrics information gathered collected, and stored?**

FAST Driver applicants that pass the initial vetting receive a call in letter from the FAST processing center. The driver will report to one of the 7 enrollment centers on the southern border or one of the 11 enrollment centers on the northern border. The drivers are interviewed, fingerprinted electronically and have their photographs taken at the

enrollment center. The digital pictures are stored electronically and the fingerprints are sent to the FBI and are not stored by CBP.

**Is the information accessible to other agencies or other entities?**

Yes. The photos and fingerprints are sent to Canadian Border Service Agency (CBSA) and the Royal Canadian Mounted Police (RCMP) through an information sharing agreement with these Canadian law enforcement agencies.

**Please describe the security measures used to protect the biometric information that is gathered, including any limitations on accessing the information.**

The information will be compliant to security measures as outlined by current OIT policy.

**At what rate have false-positives been returned during the use of biometrics in this program?**

**What is the process in place to ensure that there is not repeated false-positives in the system?**

**Did your agency conduct any privacy assessments for this use of biometrics?**

No.

**Please provide a copy of any procedures or policies your agency has in place regarding the use of biometrics. If these procedures or policies are program or initiative specific, please indicate so.**

Agency: Customs and Border Protection FAST

Contact: (b)(6)

Telephone: (b)(2), (b)(6)

E-mail: (b)(2), (b)(6)@dhs.gov

**Attachment 8  
Biometrics Survey: CBP NEXUS**

**The NEXUS Highway program** is a northern land border partnership with Canada under the Shared Border Accord, that uses two index fingerprints for identity verification.

**What is the type of biometrics technology used?**

The two index fingerprints are searched, recorded and stored in the IDENT system.

**How much did it cost your agency to implement the use of biometrics for the program/initiative and what is the FY04 projected cost for using the technology?**

Unknown.

**Is the use of biometrics for this program or initiative mandated by statute or rule? If YES, reference the statutory or regulatory citation.**

No.

**How is the biometrics information gathered, collected, and stored?**

Fingerprints are taken at enrollment, searched and stored in the IDENT system.

**Is the information accessible by other agencies or other entities (including contractors, vendors, and state and local governments)?**

The information could be made available to anyone with access to IDENT.

**Please describe the security measures used to protect the biometric information that is gathered, including any limitations on accessing the information.**

Security is done by the IDENT system.

**Did your agency conduct any privacy assessments for this use of biometrics? If so, please attach copies of any relevant assessments.**

Unknown.

**At what rate have false-positives been returned during the use of biometrics in this program?**

Unknown.

**What is the process in place to ensure that there is not repeated false-positives in the system?**

Unknown.

Agency: Customs and Border Protection

Contact: b(6)

Telephone: b(2), b(6)

E-mail: b(2), b(6) dhs.gov

**Attachment 9**  
**Biometrics Survey: CBP IDENT/IAFIS**

**Please identify the program/initiative and the purpose for using biometrics.**

The Automated Biometric Identification System and the Integrated Automated Fingerprint Identification System (IDENT/IAFIS) program.

**What is the type of biometrics technology used?**

Fingerprints and a photograph are captured. (The scanners are either Cross Match or IDENTIX scanners and the camera is a QuickCam)

**How much did it cost your agency to implement the use of biometrics for the program/initiative and what is the FY04 projected cost for using the technology?**

Congress gave the Immigration and Naturalization Service 24 million dollars in 1989 for the deployment of IDENT.

The Department of Justice was the lead on the integration of IDENT and IAFIS and Congress allocated all the money to DOJ to develop this project. (30 million)

FY04 projections including O&M money were sent forward at CBP and all funding was denied for FY04 and FY05. All funding requests for ENFORCE, which is integrated with IDENT/IAFIS, have been denied.

**Is the use of biometrics for this program or initiative mandated by statute or rule?**

The 1996 Illegal Immigration Reform and Immigrant Responsibility Act, section 326, directed the INS to expand the use of IDENT to apply to illegal or criminal aliens apprehended nationwide.

**How is the biometrics information gathered collected, and stored?**

The fingerprints are collected on either a Cross Match or IDENTIX scanner. The right and left index prints are stripped off and sent to the search against the IDENT databases and the entire set of fingerprints collected are simultaneously sent to IAFIS to query against the Criminal master File.

The fingerprints are stored locally for a total of 4-7 for a search only transaction days only. (For submission of prints for a different transaction by the user.)

Search and Enroll transactions in IDENT are stored in the Recidivist Database and if an officer enrolls someone in IAFIS, those prints are kept in the IAFIS database.

The biographical information is stored on the Enforcement Integrated Database (EID).

**Is the information accessible to other agencies or other entities?**

ICE and CIS have access to ENFORCE/IDENT/IAFIS and search and share the same information that is in the databases. The expansion of IDENT/IAFIS to allow for other state, local and federal law enforcement agencies is on going.

**Please describe the security measures used to protect the biometric information that is gathered, including any limitations on accessing the information.**

All SDLC security processes and documentation requirements were followed.

**Did your agency conduct any privacy assessments for this use of biometrics?**

Yes, and there was a Federal Register Notice announced that lawful permanent residents and United States Citizens could be queried and enrolled into IDENT/IAFIS.

Agency: Customs and Border Protection

Contact: b(6)

Telephone: b(2), b(6)

E-mail: b(2), b(6) @dhs.gov

**Attachment 10  
Biometrics Survey: CBP INSPASS**

**Please identify the program/initiative and the purpose for using biometrics.**

The Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS), is used to validate the claimed identity of travelers.

**What is the type of biometrics technology used?**

Hand geometry biometric image technology is used.

**How much did it cost your agency to implement the use of biometrics for the program/initiative and what is the FY04 projected cost for using the technology?**

Cost for implementation is unavailable at this time; however, the FY04 projected cost is approximately \$1.7million.

**Is the use of biometrics for this program or initiative mandated by statute or rule?**

No.

**How is the biometrics information gathered collected, and stored?**

The biometrics information is collected during the enrollment process and the information is stored in the Interagency Border Inspection System (IBIS).

**Is the information accessible to other agencies or other entities?**

The information is accessible by the contractor.

**Please describe the security measures used to protect the biometric information that is gathered, including any limitations on accessing the information.**

The hand geometry templates are stored in a repository for all users of the system and protected by the Privacy Act.

**Did your agency conduct any privacy assessments for this use of biometrics?**

No.

**At what rate have false-positives been returned during the use of biometrics in this program?**

None.

**What is the process in place to ensure that there is not repeated false-positives in the system?**

None.

Agency: Customs and Border Protection

Contact: b(6)

Telephone: b(2), b(6)

E-mail: b(2), b(6) @dhs.gov

CHRISTOPHER BIELE, CALIFORNIA  
 CHAIRMAN  
 MARGARET CLARK, WASHINGTON  
 VICE CHAIRMAN  
 C. W. BILL YOUNG, FLORIDA  
 BOB WOODRUFF, ALABAMA  
 F. JAMES SCHRIMMACKER, JR., WISCONSIN  
 W. J. "BOB" LINDSEY, LOUISIANA  
 DAVID DREIER, CALIFORNIA  
 DAVE LAMBERT, CALIFORNIA  
 HAROLD ROBERTS, KENTUCKY  
 BERNARDO RODRIGUEZ, NEW YORK  
 L. MARCO SWIFT, TEXAS  
 CUFFY NELSON, PENNSYLVANIA  
 CHRISTOPHER SHAYS, CONNECTICUT  
 RAYMOND J. CANNON, ILLINOIS  
 GARY CANN, INDIANA  
 NEDDY DEAN BALKENTIN, FLORIDA  
 ROBERT W. DODD, WISCONSIN  
 ANNE T. BRUCE, ALABAMA  
 P. GREG GARDNER, NEW YORK  
 JOHN LAMBERT, CALIFORNIA  
 JOHN E. BANGS, ARIZONA  
 MARK LOVORN, INDIANA  
 MAC THURMOND, TEXAS  
 PEG O'BRIEN, MISSOURI  
 LAY GARNER, TEXAS  
 PETER ROSENBERG, TEXAS  
 JOHN E. BROWNE, NEW YORK

JOHN GARDNER  
 Staff Director  
 KATHLEEN G. HINE  
 Director of the Department  
 (Health, Culture)  
 HOUSE OFFICE  
 4007 CANTON RD  
 P.O. BOX 21000



One Hundred Eighth Congress  
 U.S. House of Representatives  
 Select Committee on Homeland Security  
 Washington, DC 20515

JIM TURNER, TEXAS  
 RANKING MEMBER  
 WESLEY C. THOMPSON, MISSISSIPPI  
 CHRISTA T. SANDOZ, CALIFORNIA  
 EDWARD J. MARKEY, MASSACHUSETTS  
 NORMAN D. BOAS, WASHINGTON  
 BARRY P. RYAN, MASSACHUSETTS  
 JANE HANWAY, CALIFORNIA  
 BENJAMIN L. CARDOZ, MARYLAND  
 LOUIS H. BLAUDELTON, NEW YORK  
 PETER A. DEFAZIO, OREGON  
 BOB A. LINDSEY, NEW YORK  
 ROBERT E. JOHNSON, NEW JERSEY  
 ELIZABETH HOLLER, MONTANA  
 DISTRICT OF COLUMBIA  
 JOE LUGRELL, CALIFORNIA  
 KAREN MICHAELS, MISSOURI  
 WELLS JACKSON, TEXAS  
 BILL PASCRELL, JR., NEW JERSEY  
 DONALD H. DUBOIS, NEW JERSEY  
 BOB CHAMBERLAIN, NORTH CAROLINA  
 CHARLES A. GONZALEZ, TEXAS  
 RON LUCAS, KENTUCKY  
 JAMES J. LANGRISH, HAWAII  
 ANDREW S. BORN, FLORIDA  
 DAVID JOHNSON  
 Director of Staff Director and  
 Staff Director  
 MARK T. HOOVER  
 Director of Staff Director

March 08, 2004

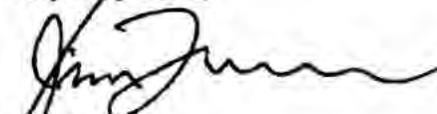
The Honorable Thomas J. Ridge  
 Secretary  
 Department of Homeland Security  
 Washington, DC 20528

Dear Secretary Ridge:

The use of biometric technologies in the government has grown significantly over the last few years, especially after the tragic events of September 11, 2001. This growth is natural as the federal government must use innovative technologies to secure our nation properly. At the same time, it is critical to our nation's security that federal agencies utilizing biometric technologies do so in a manner that protects sensitive information and individual civil liberties. As the Ranking Member of the House Select Committee on Homeland Security, I am conducting a review of how federal agencies are collecting and using biometrics collected from the general public. In addition, I am reviewing the security measures, policies, and procedures agencies have in place on such use.

Please complete the attached survey and return it to **(b)(6)** Counsel and Professional Staff for the Committee. The survey is due by March 31, 2004. If you have any questions, please feel free to contact **(b)(6)**. If your agency does not use biometrics in any of its programs, please let Jessica know that as well. Thank you for your cooperation on this matter.

Very Truly Yours,

  
 Jim Turner  
 Ranking Member



One Hundred Eighth Congress  
 U.S. House of Representatives  
 Select Committee on Homeland Security  
 Washington, DC 20515

### BIOMETRICS SURVEY – FEDERAL AGENCIES

For purposes of this survey, "biometrics" includes fingerprints, eye retinas and irises, voice patterns, DNA, and facial patterns. Please include in this survey only those biometrics programs that collect information from the general public. If your agency collects biometrics from its employees or contractors with which your agency has a professional relationship, please do not include those programs.

1. Does your agency currently collect, or plan to collect in the future, biometrics from the general public for any of its programs and initiatives? (If the answer is no, please let the Committee staff know this fact. You do not have to complete the rest of this survey).
  
2. For every program and initiative that uses biometrics technology, please answer the following questions:
  - Please identify the program/initiative and the purpose for using biometrics.
  - What is the type of biometrics technology used?
  - How much did it cost your agency to implement the use of biometrics for the program/initiative and what is the FY04 projected cost for using the technology?
  - Is the use of biometrics for this program or initiative mandated by statute or rule? If so, please explain how, or provide the statutory or regulatory citation.
  - How is the biometrics information gathered, collected, and stored?
  - Is the information accessible by other agencies or other entities (including contractors, vendors, and state and local governments)?
  - Please describe the security measures used to protect the biometric information that is gathered, including any limitations on accessing the information.
  - Did your agency conduct any privacy assessments for this use of biometrics? If so, please attach copies of any relevant assessments.
  - At what rate have false-positives been returned during the use of biometrics in this program?
  - What is the process in place to ensure that there is not repeated false-positives in the system?
  
3. Please provide a copy of any procedures or policies your agency has in place regarding the use of biometrics. If these procedures or policies are program or initiative specific, please indicate so.

Agency: \_\_\_\_\_  
 Contact: \_\_\_\_\_  
 Telephone: \_\_\_\_\_  
 E-mail: \_\_\_\_\_

Please complete this survey and return it to (b)(6) Counsel and Professional Staff, House Select Committee on Homeland Security, LA 228-Democratic Office, 101 Independence Avenue, SE, Washington, DC 20530, by MARCH 31, 2004. Alternatively, the survey can be faxed to (b)(6) attention at (b)(6).



**U.S. House of Representatives  
Select Committee on Homeland Security  
Democratic Staff**

**FACSIMILE COVER SHEET**

To: The Hon. Thomas J. Ridge

From: <sup>(b)(6)</sup> [Redacted] Select Comm. on Homeland Security, Minority Staff

Date: 3/10/04

Pages (including cover): 3

Fax Number: <sup>(b)(6)</sup> [Redacted]

Phone Number:

**Comments:**

A copy of this document will also be sent via U.S. Mail.

101 Independence Avenue, S.E.  
228 Adams Building  
Washington, D.C. 20540  
202-226-2616  
202-226-4499 (fax)

*need the  
for Turner*

DEPARTMENT OF HOMELAND SECURITY

OFFICE OF LEGISLATIVE AFFAIRS  
CONGRESSIONAL ROUTING SLIP

TRACKING NO. 2927

DUE DATE: 4/9/04

DIRECTORATE/BUREAU

- BCIS
- BTS (ICE/TSA/CBP) *cc: (b)(6)*
- MANAGEMENT *(b)(6)*
- COAST GUARD
- FEMA
  
- IAIP
  
- ODP
  
- S&T
- OLA
- OTHER



This Congressional correspondence has been forwarded to your office for a response. Please draft a response (setup for Pamela J. Turner's signature) and forward it via e-mail to *(b)(6)*. Also, provide a POC from your office on the lines below. If you have any questions, please contact the Office of Legislative Affairs at (202) 205-4412.

**IF THIS CONGRESSIONAL CORRESPONDENCE HAS BEEN MISROUTED, PLEASE NOTIFY THE OFFICE OF LEGISLATIVE AFFAIRS IMMEDIATELY.**

\_\_\_\_\_ (Name) \_\_\_\_\_ (Telephone)



# Homeland Security

JUN 14 2004

The Honorable John D. Dingell  
Ranking Member  
Committee on Energy and Commerce  
U.S. House of Representatives  
Washington, DC 20515

Dear Representative Dingell:

On behalf of Secretary Ridge, thank you for your letter regarding the deployment of radiation detection equipment and the need for funding for the Radiation Portal Monitor (RPM) program.

The priority mission of U.S. Customs and Border Protection (CBP) is to prevent radiological weapons of mass destruction (WMD) from entering this country. It is the operational goal of CBP to conduct a 100 percent radiological screening of all arriving containers, trucks, trains, cars, mail parcels, and express consignment packages.

In order to achieve this goal, CBP has implemented a risk-based priority plan for the deployment of RPMs. The CBP has been working closely with its contracted technical and scientific experts at the Pacific Northwest National Laboratory to procure the best available commercial radiation detection equipment for use as RPMs.

The CBP realizes that it cannot rely on one single process or technology to secure our borders—as a single process or technology can be defeated—and implemented a layered enforcement strategy. The CBP is developing new strategies, partnerships, and resources in order to prevent the entry of WMD. Some examples of CBP's layered enforcement strategy are the Container Security Initiative (CSI), the National Targeting Center (NTC) and Customs-Trade and Partnership Against Terrorism (C-TPAT).

The CSI allows CBP to screen cargo at foreign ports of entry, before cargo has been laden on ships coming to the United States. The NTC, through Automated Threshold Targeting, allows CBP to target all high-risk containers destined to the United States. Finally, the C-TPAT was created to engage the trade community in a cooperative relationship with CBP. The C-TPAT works with importers, carriers, brokers, and other industry sectors emphasizing a security conscious environment. The C-TPAT provides a forum in which the business community and CBP can exchange antiterrorism ideas, concepts and information, which increases the security of the entire commercial process.

As of February 2004, CBP has deployed more than 200 RPMs. The CBP will continue to deploy RPMs and other radiation detection technology to our ports of entry as quickly as possible.

In summary, CBP has accomplished much in preventing terrorists and terrorist weapons from entering the country. As the Nation's unified border agency, CBP is increasing its scrutiny of arriving conveyances and cargo at our land borders, seaports and airports. The CBP, as a key operational agency of the Department of Homeland Security, has developed ways to provide increased border security without choking off the flow of legitimate trade and travel to our country.

I appreciate your interest in the Department of Homeland Security, and I look forward to working with you on future homeland security issues. If I may be of further assistance, please contact the Office of Legislative Affairs at (202) 205-4412.

Sincerely,

A handwritten signature in cursive script, appearing to read "Pamela J. Turner".

Pamela J. Turner  
Assistant Secretary for Legislative Affairs

**Congress of the United States**  
**House of Representatives**  
**Washington, DC 20515**

March 26, 2004

The Honorable Tom Ridge  
Secretary  
Department of Homeland Security  
Washington, D.C. 20528

Dear Secretary Ridge:

As you know, we are continuing our investigation into how the U.S. Government is protecting the nation against the threat of nuclear or radiological attack. Specifically we have focused our attention on the deployment of radiation portal monitors at seaports, mail facilities, and border crossings because these devices can be used to effectively screen cargo for radiological and nuclear materials without slowing the flow of commerce.

This effort has been undertaken by the Bureau of Customs and Border Protection (CBP), under the Department of Homeland Security (DHS). CBP has a multi-phase plan to install portal monitors at designated ports of entry. The initial plan was to complete the entire installation by December 2005. While some progress has been made, considerable work remains and vulnerabilities still exist. (While we will not detail the specifics of our concerns here, a non-public attachment details our concerns further.) Under the current budget, it will be difficult, if not impossible, to meet this deadline, and we remain very concerned that this project will not receive all necessary funding.

The total cost of the project is estimated by your Department to be \$495.8 million. To date Congress has appropriated \$205.8 million to CBP for this program. In a recent meeting held with key CBP officials, staff was informed that available funding covers half of the program's phases. The Department of Homeland Security's fiscal year 2005 budget requests \$42.9 million for portal monitors. CBP staff has noted that this amount is \$247 million short of what is required to complete the installation by December 2005. According to key CBP officials significant portions of this funding is needed soon to keep this project on schedule.

Given the catastrophic impact of a major radiological or nuclear attack, these costs are comparatively trivial. We would advocate completing this project in fiscal year 2005. The failure to request these funds in your budget suggests that the Department will have significant difficulty meeting the December 2005 deadline. We would appreciate your response to the following questions about this program:

The Honorable Tom Ridge  
Page 2

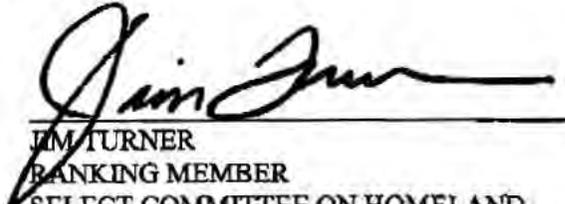
1. Does the Department intend to reprogram funds from other programs to cover the balance of the program's costs? If so, please indicate which programs would be cut to make such funds available.
2. If no reprogramming of funds is anticipated, please indicate what would be the new targeted completion date for the project if the funding level remains unchanged?

Thank you for your attention to this request. If you have any questions on this matter please contact us, or have your staff contact **(b)(6)** of the Committee on Energy and Commerce Democratic staff at **(b)(6)** or **(b)(6)** of the Select Committee on Homeland Security Democratic staff at **(b)(6)**

Sincerely,



JOHN D. DINGELL  
RANKING MEMBER  
COMMITTEE ON ENERGY AND COMMERCE



JIM TURNER  
RANKING MEMBER  
SELECT COMMITTEE ON HOMELAND SECURITY

cc: The Honorable Joe Barton, Chairman  
Committee on Energy and Commerce

The Honorable Christopher Cox, Chairman  
Select Committee on Homeland Security

**ATTACHMENT TO LETTER OF MARCH 25, 2004**  
**(Not for Public Release)**

As we stated in our letter, Customs and Border Protection (CBP) developed a six-phase deployment schedule to install monitors at the following points of entry prioritized in the following order, based on the areas CBP deemed most vulnerable:

- Phase 1: International mail facilities
- Phase 2: Major Northern Border crossings
- Phase 3: Major seaports
- Phase 4: Major Southwest Border crossings
- Phase 5: Air cargo facilities
- Phase 6: Smaller Northern Border crossings, smaller seaports, and rail border crossings.

CBP's project execution plan states all six phases will be complete by December 2005. The project's cost is \$495.8 million. To date, CBP has received \$205.8 million which would complete the first three phases: mail facilities, major northern border crossings, and major seaports. The \$42.9 million requested in 2005 would complete fifty percent of Phase 4: southern border crossings. Funding concerns have plagued this effort from the beginning. We believe that this fact has affected the overall pace of this project, and may continue to affect its rollout if not quickly addressed by your office.

Specifically, CBP has reported that the total cost of this project is approximately \$500 million. To date CBP has received approximately \$200 million. In a recent meeting held with key CBP officials, staff was informed that the expected funding milestones to complete this program would be as follows:

- \$75 million in March of 2004;
- \$75 million in June of 2004;
- \$40 million in September of 2004;
- \$50 million in December of 2004;
- \$30 million in February of 2005, and
- \$10 million in June of 2005.

At a recent meeting on this matter, CBP officials had no knowledge of where this money would come from. CBP did, however, suggest this additional funding may need to come from reprogramming of existing agency funds, which, given the amount, we find unrealistic. Staff was told that if this money is not found soon, parts of this critical homeland security project will stall. This is clearly something we cannot allow to occur. We believe that DHS should immediately reassess this effort and conduct a detailed breakout of all costs associated with the present radiation detection installation effort now underway. For this effort, DHS should also indicate specifically which phases are funded, and what phases (or sections of a phase) remain unfunded.

Our latest data indicate that portals have been installed at eighty-one percent of the mail facilities, fifty percent of the northern border crossings, and one percent of seaports. Given our continued concerns about the pace and funding of this effort, the following recommendations are being presented for your consideration:

- If additional funding will be required for any phase (which we believe it will), DHS should immediately determine a plan for obtaining and allocating this money. For example, to complete phases 5 and 6, and the unfunded balance of phase 4, DHS should determine if this money will be reprogrammed from existing CBP's programs (which CBP officials suggest will be very difficult), or from some other source. It is critical that DHS immediately determine the full income stream for completing this project and how this project will likely be affected if funds (commensurate with the above milestones) are not made available soon.
- At a minimum, we suggest that you continue receiving ongoing, detailed briefings by the U.S. General Accounting Office (who continues to conduct work in this area) on both the progress of this project and its funding needs.
- Finally, we suggest that you also pay closer attention to two other ongoing (yet closely related) efforts to identify weapons of mass destruction by CBP that we believe require serious attention. These are: (1) the Container Security Initiative program; and (2) the Customs-Trade Partnership Against Terrorism program. While both projects share laudable goals, we believe each project still lacks adequate operational structure and resources. Significant improvement in both programs is necessary before they become potent tools in the fight against terrorism.

"BUTCH" OTTER, IDAHO  
 RALPH M. MALL, TEXAS  
 MICHAEL BILIRAKIS, FLORIDA  
 FRED LUTON, MICHIGAN  
 CLIFF STEARNS, FLORIDA  
 PAUL E. GILLMOR, OHIO  
 JAMES C. GREENWOOD, PENNSYLVANIA  
 CHRISTOPHER COX, CALIFORNIA  
 NATHAN DEAL, GEORGIA  
 RICHARD BURR, NORTH CAROLINA  
 ED WHITFIELD, KENTUCKY  
 CHARLIE NORWOOD, GEORGIA  
 BARBARA CUBIN, WYOMING  
 JOHN SHIMKUS, ILLINOIS  
 HEATHER WILSON, NEW MEXICO  
 JOHN B. SHADDEG, ARIZONA  
 CHARLES W. "CHIP" PICKERING, MISSISSIPPI  
 VITO POSSELLA, NEW YORK  
 STEVE BUYER, INDIANA  
 GEORGE RADANOVICH, CALIFORNIA  
 CHARLES F. BASS, NEW HAMPSHIRE  
 JOSEPH R. PITTS, PENNSYLVANIA  
 MARY BOND, CALIFORNIA  
 GREG WALDEN, OREGON  
 LEE TERRY, NEBRASKA  
 MIKE FERGUSON, NEW JERSEY  
 MIKE ROGERS, MICHIGAN  
 DARRELL E. ISSA, CALIFORNIA  
 C.L. "BUTCH" OTTER, IDAHO  
 JOHN SULLIVAN, OKLAHOMA

BUD ALBRIGHT, STAFF DIRECTOR

ONE HUNDRED EIGHTH CONGRESS

**U.S. House of Representatives**  
**Committee on Energy and Commerce**  
**Washington, DC 20515-6115**

JOE BARTON, TEXAS  
CHAIRMAN

JOHN D. DINGELL, MICHIGAN  
 HENRY A. WAXMAN, CALIFORNIA  
 EDWARD J. MARKEY, MASSACHUSETTS  
 RICK BOUCHER, VIRGINIA  
 EDOLPHUS TOWNS, NEW YORK  
 FRANK PALLONE, JR., NEW JERSEY  
 SHERROD BROWN, OHIO  
 BART GORDON, TENNESSEE  
 PETER DEUTSCH, FLORIDA  
 BOBBY L. RUSH, ILLINOIS  
 ANNA G. ESHOO, CALIFORNIA  
 BART STUPAK, MICHIGAN  
 ELIOT L. ENGEL, NEW YORK  
 ALBERT R. WYNN, MARYLAND  
 GENE GREEN, TEXAS  
 KAREN MCCARTHY, MISSOURI  
 TED STRICKLAND, OHIO  
 DIANA DUGGETT, COLORADO  
 LOIS CAPPS, CALIFORNIA  
 MICHAEL F. DOYLE, PENNSYLVANIA  
 CHRISTOPHER JOHN, LOUISIANA  
 TOM ALLEN, MAINE  
 JIM DAVIS, FLORIDA  
 JAN SCHAKOWSKY, ILLINOIS  
 HILDA L. SOLIS, CALIFORNIA  
 CHARLES A. GONZALEZ, TEXAS

**DEMOCRATIC STAFF**

**FAX COVER SHEET**

**DATE:** 3-29-04  
**TO:** Dept. of Homeland Security Log. Affairs  
**FROM:** ETC Crisis Dem. Staff Office  
**FAX NUMBER:** 772-9734  
**NUMBER OF PAGES:** 5  
**(Including Cover)**

**COMMENTS:**  
Please see attached letter.  
Can you please forward a copy to  
the Secretary's office? Thank you.

(If there are problems with this transmission,  
 please phone 202-225-3641, Democratic Staff, 2322 RHOB.)

DEPARTMENT OF HOMELAND SECURITY

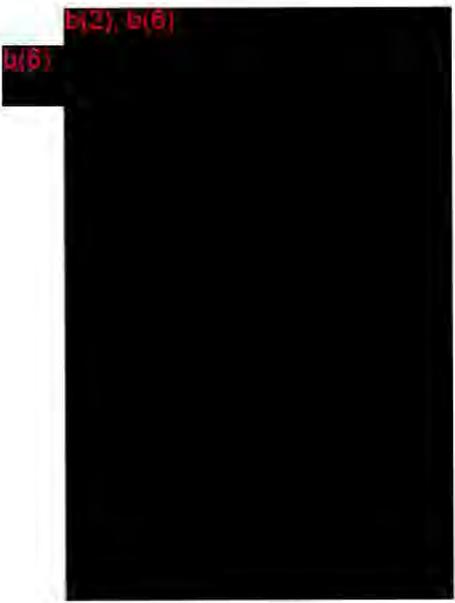
OFFICE OF LEGISLATIVE AFFAIRS  
CONGRESSIONAL ROUTING SLIP

TRACKING NO. 3073

DUE DATE: 4/13/04

DIRECTORATE/BUREAU

- BCIS
- BTS (ICE/TSA/CBP) CC:
- MANAGEMENT
- COAST GUARD
- FEMA
  
- IAIP
  
- ODP
  
- S&T
- OLA \_\_\_\_\_
- OTHER \_\_\_\_\_



This Congressional correspondence has been forwarded to your office for a response. Please draft a response (setup for Pamela J. Turner's signature) and forward it via e-mail to  Also, provide a POC from your office on the lines below. If you have any questions, please contact the Office of Legislative Affairs at (202) 205-4412.

**IF THIS CONGRESSIONAL CORRESPONDENCE HAS BEEN MISROUTED, PLEASE NOTIFY THE OFFICE OF LEGISLATIVE AFFAIRS IMMEDIATELY.**

\_\_\_\_\_ (Name) \_\_\_\_\_ (Telephone)



# Homeland Security

MAY 17 2004

The Honorable Jim Turner  
U.S. House of Representatives  
Washington, DC 20515

Dear Representative Turner:

On behalf of Secretary Ridge, thank you for your recent letter regarding the resource allocation of the bureaus of Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP) and Citizenship and Immigration Services (CIS).

Since the time of your letter, staff from the Border and Transportation Security (BTS) Directorate, CIS, and the Department's Office of the Chief Financial Officer (CFO) have briefed your staff on the circumstances and facts surrounding the *Wall Street Journal* article. The Department also established a review team composed of staff from the CFO's Office, BTS, CIS, and the U.S. Coast Guard to assess the situation. The review team engaged in a detailed budget reconciliation effort between the three bureaus. The team examined the allocation of resources and services throughout the three bureaus, and this effort resulted in an immediate internal realignment of \$212 million. A subsequent internal realignment of approximately \$270 million is possible, pending additional discussions and coordination on the final documentation and billing. There is no \$1.2 billion shortfall as reported by the *Wall Street Journal*.

The Congress has recognized that funds may need to be realigned between ICE, CBP, and CIS. In the Joint Explanatory Statement (H. Rpt. 108-280) accompanying the Department of Homeland Security Appropriations Act, 2004 (P.L. 108-90), the Congress recognized that the budgetary resources may need to be realigned. Specifically, the Congress noted: *"The conferees are aware that the Department is conducting a comprehensive review of administrative and other mission responsibilities, particularly as they affect ICE and other agencies that have inherited multiple legacy missions. While funding provided by this conference agreement is based on the best possible information available, the conferees understand there may be a need to adjust funding to conform to the decisions resulting from the review."* A similar statement was included under the heading discussing CBP.

Over the past year, these three bureaus have undergone major successful reorganizations by incorporating programs, staff, and resources from legacy programs at the Immigration and Naturalization Service and the U.S. Customs Service (as well as General Services Administration and the Department of Agriculture) and a realignment of functions to strengthen the security of the nation. Through this process, which included successful reassignment of over 50,000 employees from the legacy agencies, robust hiring continued to ensure adequate staffing to accomplish mission objectives. However, the transformation effort has not been

without challenges, and each bureau continues to integrate everything from budgets to uniforms to Standard Operating Procedures in virtually every area. The Department has made great progress to date.

During a review of the status of execution of the FY 2004 budget, ICE and CBP determined that implementation of hiring restrictions was a prudent managerial measure not just to stay within 2004 appropriations, but for mission-related objectives. CIS had already instituted hiring restrictions since the beginning of the fiscal year due to lower than anticipated fee projections. Additional focus was, and is, required to work through funding realignments related to the establishment of the three new bureaus. This work recognized the tremendous effort of the Administration and the Congress to establish the Department but also acknowledged that some of the finer details on funding and provision of support services required negotiations and reconciliation between the three bureaus. The work has been ongoing, and agreements have been recently reached to realign funds to cover costs of services incurred by the bureaus. Formal memoranda of agreement will be implemented between the three bureaus, which will align funding with services rendered.

The Department is committed to the security of the nation, and it will continue to work toward successful operation of the three bureaus, CBP, CIS, and ICE. To that end, DHS will continue to work with the Congress, to ensure that funds are aligned to mission objectives and are consistent with Congressional intent.

I appreciate your interest in the Department of Homeland Security, and I look forward to working with you on future homeland security issues. If you need further assistance, please contact the Office of Legislative Affairs at (202) 205-4412.

Sincerely,

A handwritten signature in black ink, appearing to read "Pam Turner", with a stylized flourish at the end.

Pamela J. Turner  
Assistant Secretary for Legislative Affairs

645

CHRISTOPHER COX, CALIFORNIA  
CHAIRMAN

JENNIFER DUNN, WASHINGTON,  
VICE CHAIRMAN

C.W. BILL YOUNG, FLORIDA

DON YOUNG, ALASKA

F. JAMES SENSENBRENNER, JR., WISCONSIN

W.J. "BILLY" TALZIN, LOUISIANA

DAVID DREIER, CALIFORNIA

DUNCAN HUNTER, CALIFORNIA

HAROLD ROGERS, KENTUCKY

SHERWOOD BOEHLERT, NEW YORK

LAMAR SMITH, TEXAS

CURT WELDON, PENNSYLVANIA

CHRISTOPHER SHAYS, CONNECTICUT

PORTER J. GOSS, FLORIDA

DAVE CAMP, MICHIGAN

LINDOLN DIAZ-BALART, FLORIDA

ROBERT W. GOODLATTE, VIRGINIA

ERNEST J. ISTOOK, JR., OKLAHOMA

PETER T. KING, NEW YORK

JOHN LINDER, GEORGIA

JOHN B. SHADDEG, ARIZONA

MARK SOLDER, INDIANA

MAC THORNBERY, TEXAS

JIM GIBBONS, NEVADA

KAY GRANGER, TEXAS

PETE SESSIONS, TEXAS

JOHN E. SWEENEY, NEW YORK



One Hundred Eighth Congress  
 U.S. House of Representatives  
 Select Committee on Homeland Security  
 Washington, DC 20515

March 26, 2004

JIM TURNER, TEXAS,  
RANKING MEMBER

BENNE G. THOMPSON, MISSISSIPPI

LORETTA T. SANCHEZ, CALIFORNIA

EDWARD J. MARKEY, MASSACHUSETTS

NORMAN D. DICKS, WASHINGTON

BARNEY FRANK, MASSACHUSETTS

JANE HARMAN, CALIFORNIA

BENJAMIN L. CARDIN, MARYLAND

LOUISE M. BLALOCK, NEW YORK

PETER A. DEFAZZO, OREGON

MITA M. LOWEY, NEW YORK

ROBERT E. ANDREWS, NEW JERSEY

ELIZABETH HOLMES NORTON,  
DISTRICT OF COLUMBIA

ZOE LOFGREEN, CALIFORNIA

KAREN MCCARTHY, MISSOURI

SHENIA JACKSON-LEE, TEXAS

BILL PASCRELL, JR., NEW JERSEY

DONNA M. CHRISTENSEN, U.S. VIRGIN ISLANDS

BOB ETHERIDGE, NORTH CAROLINA

CHARLES A. GONZALEZ, TEXAS

REN LUCAS, KENTUCKY

JAMES R. LANGEVIN, RHODE ISLAND

KENDRICK B. MEER, FLORIDA

DAVID SCHANZER  
 DEMOCRATIC STAFF DIRECTOR AND  
 CHIEF COUNSEL

MARK T. MAGEE  
 DEMOCRATIC DEPUTY STAFF DIRECTOR

JOHN GANNON  
 STAFF DIRECTOR

STEPHEN DEYNE  
 DEPUTY STAFF DIRECTOR AND  
 GENERAL COUNSEL

THOMAS DLENGE  
 CHIEF COUNSEL AND  
 POLICY DIRECTOR

The Honorable Tom Ridge  
 Department of Homeland Security  
 Washington, D.C. 20528

Dear Secretary Ridge:

Today, the *Wall Street Journal* reported that a potential budget shortfall of \$1.2 billion has resulted in a hiring freeze affecting the Bureaus of Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE). A hiring freeze has also been instituted at the Bureau of Citizenship and Immigration Services (CIS). All of these entities perform front-line missions critical to securing our nation.

Specifically, the *Wall Street Journal* article stated that a \$1.2 billion shortfall exists within the budgets of ICE and CBP, representing 12.3% of the total funding for both agencies. If this is the case, and the hiring freeze must be maintained, our nation's security could be significantly impacted.

It is important for the Select Committee to have a full understanding of any budget pressures facing the DHS. I request that you immediately provide the Select Committee with a detailed assessment of whether the \$1.2 billion budget shortfall exists, the reasons for its existence, potential remediation efforts, and the impact of such efforts -- as well as the current personnel hiring freeze -- on security measures at our nation's borders, sea ports and airways. The Select Committee stands ready to provide assistance to the DHS, but finds it inconsistent with the oversight responsibility of the Select Committee to learn of significant hiring freezes or budget shortfalls from a newspaper article. The point of contact on my staff on this issue is David Schanzer, 202-226-2616.

Sincerely,

Jim Turner  
 Ranking Member

cc: The Honorable Christopher Cox

DEPARTMENT OF HOMELAND SECURITY

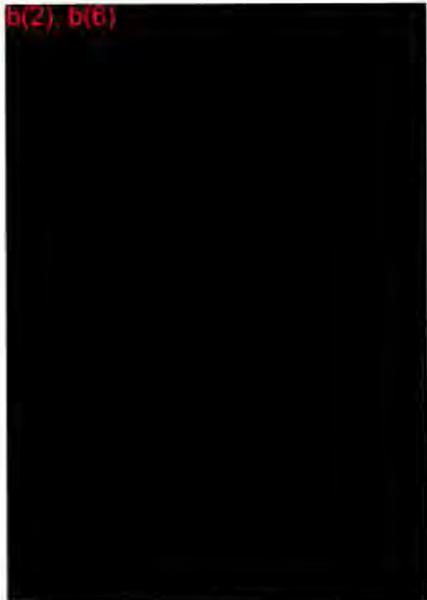
OFFICE OF LEGISLATIVE AFFAIRS  
CONGRESSIONAL ROUTING SLIP

TRACKING NO. 3187

DUE DATE: 4/23/04

DIRECTORATE/BUREAU

- BCIS
- BTS (ICE/TSA/CBP)
- MANAGEMENT
- COAST GUARD
- FEMA
  
- IAIP
  
- ODP
  
- S&T
- OLA \_\_\_\_\_
- OTHER \_\_\_\_\_



This Congressional correspondence has been forwarded to your office for a response. Please draft a response (setup for Pamela J. Turner's signature) and forward it via e-mail to b(6). Also, provide a POC from your office on the lines below. If you have any questions, please contact the Office of Legislative Affairs at (202) 205-4412.

**IF THIS CONGRESSIONAL CORRESPONDENCE HAS BEEN MISROUTED, PLEASE NOTIFY THE OFFICE OF LEGISLATIVE AFFAIRS IMMEDIATELY.**

\_\_\_\_\_ (Name)

\_\_\_\_\_ (Telephone)

b(6)

---

**From:** b(6)  
**Sent:** Friday, April 16, 2004 2:32 PM  
**To:** b(6)  
**Subject:** reassign 3182

Please reassign LA 3182( BTS 4746) to Management. See below email.

-----Original Message-----

**From:** b(6)  
**Sent:** Friday, April 16, 2004 2:11 PM  
**To:** b(6)  
**Cc:** b(6)  
**Subject:** RE: congressional BTS 4746

Why aren't these going to U/S for Mgmnt CFO given that it is ICE/CBP and CIS and they are the WG lead?



# Homeland Security

MAY 17 2004

The Honorable Jim Turner  
U.S. House of Representatives  
Washington, DC 20515

Dear Representative Turner:

On behalf of Secretary Ridge, thank you for your recent letter regarding the resource allocation of the bureaus of Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP) and Citizenship and Immigration Services (CIS).

Since the time of your letter, staff from the Border and Transportation Security (BTS) Directorate, CIS, and the Department's Office of the Chief Financial Officer (CFO) have briefed your staff on the circumstances and facts surrounding the *Wall Street Journal* article. The Department also established a review team composed of staff from the CFO's Office, BTS, CIS, and the U.S. Coast Guard to assess the situation. The review team engaged in a detailed budget reconciliation effort between the three bureaus. The team examined the allocation of resources and services throughout the three bureaus, and this effort resulted in an immediate internal realignment of \$212 million. A subsequent internal realignment of approximately \$270 million is possible, pending additional discussions and coordination on the final documentation and billing. There is no \$1.2 billion shortfall as reported by the *Wall Street Journal*.

The Congress has recognized that funds may need to be realigned between ICE, CBP, and CIS. In the Joint Explanatory Statement (H. Rpt. 108-280) accompanying the Department of Homeland Security Appropriations Act, 2004 (P.L. 108-90), the Congress recognized that the budgetary resources may need to be realigned. Specifically, the Congress noted: *"The conferees are aware that the Department is conducting a comprehensive review of administrative and other mission responsibilities, particularly as they affect ICE and other agencies that have inherited multiple legacy missions. While funding provided by this conference agreement is based on the best possible information available, the conferees understand there may be a need to adjust funding to conform to the decisions resulting from the review."* A similar statement was included under the heading discussing CBP.

Over the past year, these three bureaus have undergone major successful reorganizations by incorporating programs, staff, and resources from legacy programs at the Immigration and Naturalization Service and the U.S. Customs Service (as well as General Services Administration and the Department of Agriculture) and a realignment of functions to strengthen the security of the nation. Through this process, which included successful reassignment of over 50,000 employees from the legacy agencies, robust hiring continued to ensure adequate staffing to accomplish mission objectives. However, the transformation effort has not been

without challenges, and each bureau continues to integrate everything from budgets to uniforms to Standard Operating Procedures in virtually every area. The Department has made great progress to date.

During a review of the status of execution of the FY 2004 budget, ICE and CBP determined that implementation of hiring restrictions was a prudent managerial measure not just to stay within 2004 appropriations, but for mission-related objectives. CIS had already instituted hiring restrictions since the beginning of the fiscal year due to lower than anticipated fee projections. Additional focus was, and is, required to work through funding realignments related to the establishment of the three new bureaus. This work recognized the tremendous effort of the Administration and the Congress to establish the Department but also acknowledged that some of the finer details on funding and provision of support services required negotiations and reconciliation between the three bureaus. The work has been ongoing, and agreements have been recently reached to realign funds to cover costs of services incurred by the bureaus. Formal memoranda of agreement will be implemented between the three bureaus, which will align funding with services rendered.

The Department is committed to the security of the nation, and it will continue to work toward successful operation of the three bureaus, CBP, CIS, and ICE. To that end, DHS will continue to work with the Congress, to ensure that funds are aligned to mission objectives and are consistent with Congressional intent.

I appreciate your interest in the Department of Homeland Security, and I look forward to working with you on future homeland security issues. If you need further assistance, please contact the Office of Legislative Affairs at (202) 205-4412.

Sincerely,

A handwritten signature in black ink, appearing to read "Pam Turner", with a stylized flourish at the end.

Pamela J. Turner  
Assistant Secretary for Legislative Affairs

645

CHRISTOPHER COX, CALIFORNIA  
CHAIRMAN

JENNIFER DUNN, WASHINGTON,  
VICE CHAIRMAN

C.W. BILL YOUNG, FLORIDA

DON YOUNG, ALASKA

F. JAMES SENSENBRENNER, JR., WISCONSIN

W.J. "BILLY" TALZIN, LOUISIANA

DAVID DREIER, CALIFORNIA

DUNCAN HUNTER, CALIFORNIA

HAROLD ROGERS, KENTUCKY

SHERWOOD BOEHLERT, NEW YORK

LAMAR SMITH, TEXAS

CURT WELDON, PENNSYLVANIA

CHRISTOPHER SHAYS, CONNECTICUT

PORTER J. GOSS, FLORIDA

DAVE CAMP, MICHIGAN

LINDOLN DIAZ-BALART, FLORIDA

ROBERT W. GOODLATTE, VIRGINIA

ERNEST J. ISTOOK, JR., OKLAHOMA

PETER T. KING, NEW YORK

JOHN LINDER, GEORGIA

JOHN B. SHADDEG, ARIZONA

MARK SOLDER, INDIANA

MAC THORNBERY, TEXAS

JIM GIBBONS, NEVADA

KAY GRANGER, TEXAS

PETE SESSIONS, TEXAS

JOHN E. SWEENEY, NEW YORK



One Hundred Eighth Congress  
 U.S. House of Representatives  
 Select Committee on Homeland Security  
 Washington, DC 20515

March 26, 2004

JIM TURNER, TEXAS,  
RANKING MEMBER

BENNE G. THOMPSON, MISSISSIPPI

LORETTA T. SANCHEZ, CALIFORNIA

EDWARD J. MARKEY, MASSACHUSETTS

NORMAN D. DICKS, WASHINGTON

BARNEY FRANK, MASSACHUSETTS

JANE HARMAN, CALIFORNIA

BENJAMIN L. CARDIN, MARYLAND

LOUISE M. BLALOCK, NEW YORK

PETER A. DEFAZZO, OREGON

MITA M. LOWEY, NEW YORK

ROBERT E. ANDREWS, NEW JERSEY

ELIZABETH HOLMES NORTON,  
DISTRICT OF COLUMBIA

ZOE LOFGREEN, CALIFORNIA

KAREN MCCARTHY, MISSOURI

SHENIA JACKSON-LEE, TEXAS

BILL PASCRELL, JR., NEW JERSEY

DONNA M. CHRISTENSEN, U.S. VIRGIN ISLANDS

BOB ETHERIDGE, NORTH CAROLINA

CHARLES A. GONZALEZ, TEXAS

REN LUCAS, KENTUCKY

JAMES R. LANGEVIN, RHODE ISLAND

KENDRICK B. MEER, FLORIDA

DAVID SCHANZER  
 DEMOCRATIC STAFF DIRECTOR AND  
 CHIEF COUNSEL

MARK T. MAGEE  
 DEMOCRATIC DEPUTY STAFF DIRECTOR

JOHN GANNON  
 STAFF DIRECTOR

STEPHEN DEYNE  
 DEPUTY STAFF DIRECTOR AND  
 GENERAL COUNSEL

THOMAS DLENGE  
 CHIEF COUNSEL AND  
 POLICY DIRECTOR

The Honorable Tom Ridge  
 Department of Homeland Security  
 Washington, D.C. 20528

Dear Secretary Ridge:

Today, the *Wall Street Journal* reported that a potential budget shortfall of \$1.2 billion has resulted in a hiring freeze affecting the Bureaus of Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE). A hiring freeze has also been instituted at the Bureau of Citizenship and Immigration Services (CIS). All of these entities perform front-line missions critical to securing our nation.

Specifically, the *Wall Street Journal* article stated that a \$1.2 billion shortfall exists within the budgets of ICE and CBP, representing 12.3% of the total funding for both agencies. If this is the case, and the hiring freeze must be maintained, our nation's security could be significantly impacted.

It is important for the Select Committee to have a full understanding of any budget pressures facing the DHS. I request that you immediately provide the Select Committee with a detailed assessment of whether the \$1.2 billion budget shortfall exists, the reasons for its existence, potential remediation efforts, and the impact of such efforts -- as well as the current personnel hiring freeze -- on security measures at our nation's borders, sea ports and airways. The Select Committee stands ready to provide assistance to the DHS, but finds it inconsistent with the oversight responsibility of the Select Committee to learn of significant hiring freezes or budget shortfalls from a newspaper article. The point of contact on my staff on this issue is David Schanzer, 202-226-2616.

Sincerely,

Jim Turner  
 Ranking Member

cc: The Honorable Christopher Cox

DEPARTMENT OF HOMELAND SECURITY

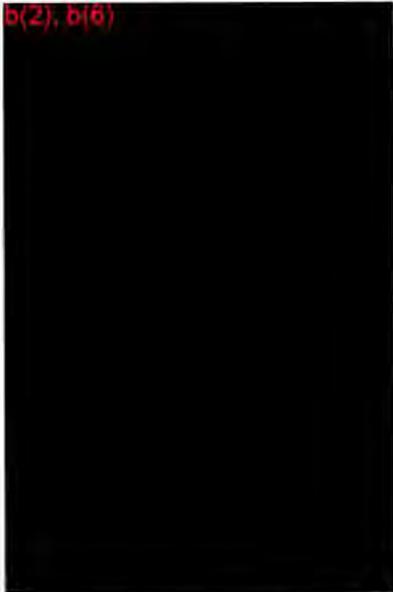
OFFICE OF LEGISLATIVE AFFAIRS  
CONGRESSIONAL ROUTING SLIP

TRACKING NO. 3187

DUE DATE: 4/23/04

DIRECTORATE/BUREAU

- BCIS
- BTS (ICE/TSA/CBP)
- MANAGEMENT
- COAST GUARD
- FEMA
  
- IAIP
  
- ODP
  
- S&T
- OLA \_\_\_\_\_
- OTHER \_\_\_\_\_



This Congressional correspondence has been forwarded to your office for a response. Please draft a response (setup for Pamela J. Turner's signature) and forward it via e-mail to **b(6)**. Also, provide a POC from your office on the lines below. If you have any questions, please contact the Office of Legislative Affairs at (202) 205-4412.

**IF THIS CONGRESSIONAL CORRESPONDENCE HAS BEEN MISROUTED, PLEASE NOTIFY THE OFFICE OF LEGISLATIVE AFFAIRS IMMEDIATELY.**

\_\_\_\_\_ (Name)

\_\_\_\_\_ (Telephone)

b(6)

---

**From:** b(6)  
**Sent:** Friday, April 16, 2004 2:32 PM  
**To:** b(6)  
**Subject:** reassign 3182

Please reassign LA 3182( BTS 4746) to Management. See below email.

-----Original Message-----

**From:** b(6)  
**Sent:** Friday, April 16, 2004 2:11 PM  
**To:** b(6)  
**Cc:** b(6)  
**Subject:** RE: congressional BTS 4746

Why aren't these going to U/S for Mgmnt CFO given that it is ICE/CBP and CIS and they are the WG lead?

DEPARTMENT OF HOMELAND SECURITY

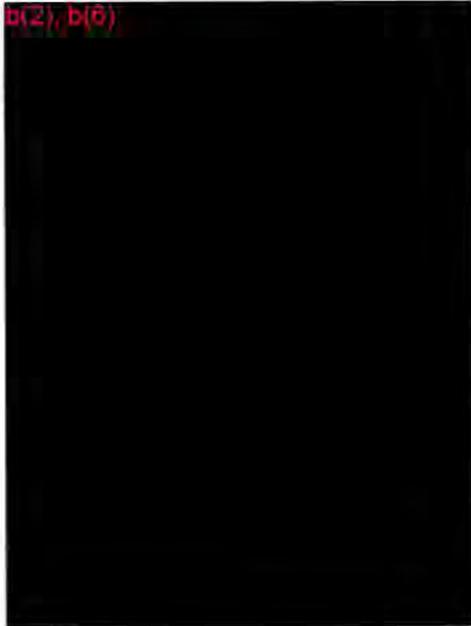
OFFICE OF LEGISLATIVE AFFAIRS  
CONGRESSIONAL ROUTING SLIP

TRACKING NO. 4663

DUE DATE: 10/4/04

DIRECTORATE/BUREAU

- BCIS
- BTS (ICE/TSA/CBP) CC:
- MANAGEMENT
- COAST GUARD
- FEMA
  
- IAIP
  
- ODP
  
- S&T
- OLA
- OTHER



This Congressional correspondence has been forwarded to your office for a response. Please draft a response (setup for Pamela J. Turner's signature) and forward it via e-mail to [Congressionalcorrespondence@dhs.gov](mailto:Congressionalcorrespondence@dhs.gov). Also, provide a POC from your office on the lines below. If you have any questions, please contact the Office of Legislative Affairs at (202) 205-4412.

IF THIS CONGRESSIONAL CORRESPONDENCE HAS BEEN MISROUTED, PLEASE NOTIFY THE OFFICE OF LEGISLATIVE AFFAIRS IMMEDIATELY.

\_\_\_\_\_ (Name)

\_\_\_\_\_ (Telephone)

**Congress of the United States**  
**Washington, DC 20515**

September 14, 2004

The Honorable Tom Ridge  
Secretary  
U.S. Department of Homeland Security  
Washington, DC 20528

Dear Secretary Ridge:

According to recent media reports, the Transportation Security Administration (TSA) has begun to require new security measures for direct flights from Moscow to the United States. We are particularly interested in one of the new TSA security mandates for these flights: inspection of all air cargo onboard for the presence of explosives and other dangerous materials.

As you know, the recent turmoil in Russia, including the two downed flights on August 24, the horrific hostage situation in Beslan, and the terrorist bombing of a Russian subway station on August 31, indicate a need for heightened efforts to thwart terrorist attacks in that country. Because of the potential that terrorism in Russia could impact the United States and its citizens, we fully support TSA's efforts to tighten security on inbound flights from Russia.

We read with great interest that TSA now reportedly requires full cargo inspections on these flights, and we would like more information on how this screening is being conducted. As you know, the lack of full screening of cargo on passenger aircraft arriving at and departing from U.S. airports remains one of the most, if not *the* most, glaring security vulnerabilities in air travel today. We have included a series of questions below on TSA's cargo screening policies and procedures for these flights, and appreciate the Department's prompt response to these questions.

Additionally, according to press accounts, TSA has mandated enhanced screening of passengers and their baggage for explosives on these flights. We are interested in how this screening is to take place, given the continuing inability to routinely screen passengers on U.S. flights for such concealed explosives.

Please respond to the following questions:

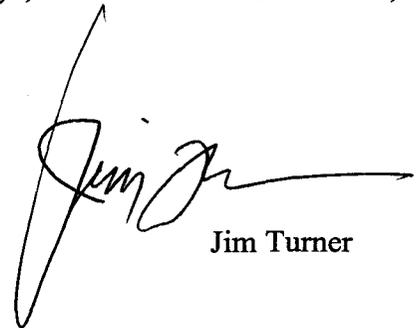
1. Given TSA's efforts to prioritize resources, on what basis were the Russian flights designated as having a greater need for full cargo screening than any other arriving international or domestic flight? Are there any other instances in which TSA is currently conducting full screening of all the cargo onboard? If not, why does TSA consider other routes less of a risk, from a security standpoint, and therefore not in need of 100% cargo screening? Has TSA considered implementing 100% cargo screening on other routes or particular flights? If yes, which ones?

2. Who is responsible for screening the cargo on the Delta and Aeroflot Russian Airline flights? Does TSA have any personnel at the airport to oversee the cargo screening operations? If not, why not?
3. Considering the argument put forth by TSA and the Directorate for Border and Transportation Security that technology does not exist to screen 100% of air cargo loaded on passenger planes, which method(s) are being used to screen cargo on these flights? What specific technology, if any, is being used to screen the cargo on the Delta and Aeroflot Russian Airline flights?
4. According to a response by former Assistant Administrator McHale at a Homeland Security Committee hearing on May 12, 2004, "We do not screen every single piece of cargo that could be screened today by technology." That is, even absent the argument that technology does not exist, there is still cargo on passenger planes that could be, but is not, physically screened. Why?
5. Earlier this year, TSA announced it would require air carriers to conduct random physical inspections of cargo carried on passenger planes which, in turn, would be randomly verified by TSA. Since the beginning of this policy, how many inspections have the air carriers conducted? Please provide a list, by carrier, that indicates the date of each of these inspections. How many verifications of these inspections has TSA conducted? Please provide a list which includes the date of each verification and the carrier involved.
6. Since TSA began conducting verifications, how many instances have there been in which carriers have failed the verification? What are the consequences for carriers who fail the verification, if any? How many TSA personnel are responsible for conducting the verifications?

We appreciate your responses to these questions regarding passenger and cargo screening, and stand ready to support effective policies that you may propose to improve the security of our aviation industry. Please provide responses within 15 business days, or no later than October 16, 2004.

Sincerely,

  
Edward J. Markey

  
Jim Turner

cc:  
Admiral David Stone  
Administrator  
Transportation Security Administration  
601 South 12th Street  
Arlington, VA 22202-4220



MAR 04 2007

**Homeland  
Security**

The Honorable Edward J. Markey  
U.S. House of Representatives  
Washington, DC 20515

Dear Representative Markey:

On behalf of Secretary Chertoff, thank you for your letter, regarding new security measures for direct flights from Moscow to the United States. The following information is provided in response to your questions.

In the best interests of foreign relations, special protection is afforded to information received during foreign airport assessments and air carrier inspections, and this information is classified in accordance with Executive Order 12958 regarding National Security Information. This response does not include certain relevant information that is Sensitive Security Information. Should more specific information be required, the Transportation Security Administration (TSA) is prepared to provide you with a private briefing.

1. Question: Given TSA's efforts to prioritize resources, on what basis were the Russian flights designated as having a greater need for full cargo screening than any other arriving international or domestic flight? Are there any other instances in which TSA is currently conducting full screening of all the cargo onboard? If not, why does TSA consider other routes less of a risk, from a security standpoint, and therefore not in need of 100 percent cargo screening? Has TSA considered implementing 100 percent cargo screening on other routes or particular flights? If yes, which ones?

Response: The downing of two Russian commercial flights, coupled with other terrorist attacks on Russian targets, prompted the need for additional security measures to be placed on flights originating from Russia and arriving in the United States. TSA has directed, in the past, similar enhancements to aviation security on other routes to/from the United States, most notably during the 2003 Holiday Season when the Homeland Security Threat Advisory Level was raised to Orange.

2. Question: Who is responsible for screening the cargo on the Delta and Aeroflot Russian Airline flights? Does TSA have any personnel at the airport to oversee the cargo screening operations? If not, why not?

Response: Both Aeroflot and Delta Airlines screen cargo in accordance with TSA air carrier security program requirements, security directives, and the Russian National Civil Aviation Security Program. This is accomplished in conjunction with the Russian State Civil Aviation Service to ensure that cargo intended for carriage on passenger flights has

been subjected to appropriate security controls as outlined in the International Civil Aviation Organization (ICAO) Annex 17 Standards and Recommended Practices.

In accordance with the Aviation and Transportation Security Act, TSA Aviation Security Inspectors, specially trained in international operations, routinely perform foreign airport assessments, air carrier inspections, and special security deployments, e.g., Secretarial actions, special events, and specific threats to aviation on a worldwide basis.

Immediately following the attacks on Russian civil aviation, TSA deployed personnel to Russia to analyze threat information and identify vulnerabilities associated with the threat so that adequate risk mitigation measures could be developed. These personnel remain available for re-deployment should the need arise and maintain an ongoing dialogue with colleagues from the Russian State Civil Aviation Service.

3. Question: Considering the argument put forth by TSA and the Directorate for Border and Transportation Security that technology does not exist to screen 100 percent of air cargo loaded on passenger planes, which methods(s) are being used to screen cargo on these flights? What specific technology, if any, is being used to screen the cargo on the Delta and Aeroflot Russian Airline flights?

Response: The Russian State Civil Aviation Service uses a combination of technological and physical security countermeasures, to include X-ray screening, physical searches, and other appropriate security controls.

4. Question: According to a response by former Assistant Administrator McHale at a Homeland Security Committee hearing on May 12, 2004, "We do not screen every single piece of cargo that could be screened today by technology." That is, even absent the argument that technology does not exist; there is still cargo on passenger planes that could be, but is not, physically screened. Why?

Response: Given the enormity of the task regarding cargo screening and security, the foundation of TSA's approach is to work in close partnership with aviation industry stakeholders, Congress, and other federal agencies both within and outside of the Department of Homeland Security. TSA continues to strive to develop and implement a layered solution that improves security by eliminating dangerous single points of failure while preserving the high value air cargo supply chain. A critical component of achieving this goal is the development and deployment of the Air Cargo Freight Assessment System (FAS), which TSA is currently developing in coordination with CBP. The FAS will build on existing risk assessment tools within the Department, including those in the Automated Commercial Environment, to effectively target high-risk air cargo. Air carriers will then be required to inspect 100% of shipments identified as high risk by the FAS. Through this combination of prescreening and inspection, DHS expects to achieve security gains that equal or exceed those possible through an inspection regime based on an arbitrary percentage rate, without impeding commerce. These layers of protection in cargo security will become even stronger as the Air Cargo Strategic Plan, the recently published notice of proposed rulemaking, and other initiatives are pursued.

5. Question: Earlier this year, TSA announced it would require air carriers to conduct random physical inspections of cargo carried on passenger planes which, in turn, would be randomly verified by TSA. Since the beginning of this policy, how many inspections have the air carriers conducted? Please provide a list, by carrier, that indicates the date of each of these inspections. How many verifications of these inspections has TSA conducted? Please provide a list that includes the date of each verification and the carrier involved.

Response: Air carriers do not report cargo screening data to TSA; therefore, TSA does not have records which indicate the number of times air carriers have screened cargo, nor the locations and dates of that screening. TSA Aviation Security Inspectors do perform compliance inspections in order to verify the air carriers are properly screening air cargo. According to the TSA inspection database, as of January 24, 2005, TSA has conducted at least 11,091 such compliance inspections related to air cargo screening at various domestic airports.

6. Question: Since TSA began conducting verifications, how many instances have there been in which carriers have failed the verifications? What are the consequences for carriers who fail the verifications, if any? How many TSA personnel are responsible for conducting the verifications?

Response: Since the initiation of the cargo screening policy, TSA has documented an extremely low number of compliance deficiencies related to cargo screening, estimated to be less than 1 or 2%. Consequences for failing to comply with TSA cargo screening requirements include counseling, administrative action, or civil penalty action. TSA currently has 100 Aviation Security Inspectors who are dedicated to ensuring compliance with air cargo security measures. These inspectors are augmented by 729 other Aviation Security Inspectors who are responsible for verifying overall air carrier compliance with aviation security requirements, including air cargo requirements.

I appreciate your interest in the Department of Homeland Security, and I look forward to working with you on future homeland security issues. If I may be of further assistance, please contact the Office of Legislative Affairs at (202) 205-4412.

Sincerely,



Pamela J. Turner  
Assistant Secretary for Legislative Affairs

**Congress of the United States**  
**Washington, DC 20515**

September 14, 2004

The Honorable Tom Ridge  
Secretary  
U.S. Department of Homeland Security  
Washington, DC 20528

Dear Secretary Ridge:

According to recent media reports, the Transportation Security Administration (TSA) has begun to require new security measures for direct flights from Moscow to the United States. We are particularly interested in one of the new TSA security mandates for these flights: inspection of all air cargo onboard for the presence of explosives and other dangerous materials.

As you know, the recent turmoil in Russia, including the two downed flights on August 24, the horrific hostage situation in Beslan, and the terrorist bombing of a Russian subway station on August 31, indicate a need for heightened efforts to thwart terrorist attacks in that country. Because of the potential that terrorism in Russia could impact the United States and its citizens, we fully support TSA's efforts to tighten security on inbound flights from Russia.

We read with great interest that TSA now reportedly requires full cargo inspections on these flights, and we would like more information on how this screening is being conducted. As you know, the lack of full screening of cargo on passenger aircraft arriving at and departing from U.S. airports remains one of the most, if not *the* most, glaring security vulnerabilities in air travel today. We have included a series of questions below on TSA's cargo screening policies and procedures for these flights, and appreciate the Department's prompt response to these questions.

Additionally, according to press accounts, TSA has mandated enhanced screening of passengers and their baggage for explosives on these flights. We are interested in how this screening is to take place, given the continuing inability to routinely screen passengers on U.S. flights for such concealed explosives.

Please respond to the following questions:

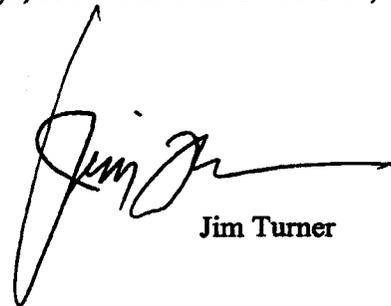
1. Given TSA's efforts to prioritize resources, on what basis were the Russian flights designated as having a greater need for full cargo screening than any other arriving international or domestic flight? Are there any other instances in which TSA is currently conducting full screening of all the cargo onboard? If not, why does TSA consider other routes less of a risk, from a security standpoint, and therefore not in need of 100% cargo screening? Has TSA considered implementing 100% cargo screening on other routes or particular flights? If yes, which ones?

2. Who is responsible for screening the cargo on the Delta and Aeroflot Russian Airline flights? Does TSA have any personnel at the airport to oversee the cargo screening operations? If not, why not?
3. Considering the argument put forth by TSA and the Directorate for Border and Transportation Security that technology does not exist to screen 100% of air cargo loaded on passenger planes, which method(s) are being used to screen cargo on these flights? What specific technology, if any, is being used to screen the cargo on the Delta and Aeroflot Russian Airline flights?
4. According to a response by former Assistant Administrator McHale at a Homeland Security Committee hearing on May 12, 2004, "We do not screen every single piece of cargo that could be screened today by technology." That is, even absent the argument that technology does not exist, there is still cargo on passenger planes that could be, but is not, physically screened. Why?
5. Earlier this year, TSA announced it would require air carriers to conduct random physical inspections of cargo carried on passenger planes which, in turn, would be randomly verified by TSA. Since the beginning of this policy, how many inspections have the air carriers conducted? Please provide a list, by carrier, that indicates the date of each of these inspections. How many verifications of these inspections has TSA conducted? Please provide a list which includes the date of each verification and the carrier involved.
6. Since TSA began conducting verifications, how many instances have there been in which carriers have failed the verification? What are the consequences for carriers who fail the verification, if any? How many TSA personnel are responsible for conducting the verifications?

We appreciate your responses to these questions regarding passenger and cargo screening, and stand ready to support effective policies that you may propose to improve the security of our aviation industry. Please provide responses within 15 business days, or no later than October 16, 2004.

Sincerely,

  
Edward J. Markey

  
Jim Turner

cc:  
Admiral David Stone  
Administrator  
Transportation Security Administration  
601 South 12th Street  
Arlington, VA 22202-4220

DEPARTMENT OF HOMELAND SECURITY

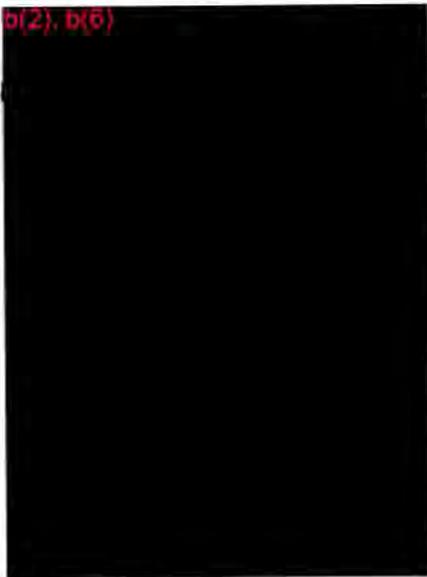
OFFICE OF LEGISLATIVE AFFAIRS  
CONGRESSIONAL ROUTING SLIP

TRACKING NO. 4663/22875

DUE DATE: 10/4/04

DIRECTORATE/BUREAU

- BCIS
- BTS (ICE/TSA/CBP) cc:
- MANAGEMENT
- COAST GUARD
- FEMA
  
- IAIP
  
- ODP
  
- S&T
- OLA \_\_\_\_\_
- OTHER \_\_\_\_\_



This Congressional correspondence has been forwarded to your office for a response. Please draft a response (setup for Pamela J. Turner's signature) and forward it via e-mail to [Congressionalcorrespondence@dhs.gov](mailto:Congressionalcorrespondence@dhs.gov). Also, provide a POC from your office on the lines below. If you have any questions, please contact the Office of Legislative Affairs at (202) 205-4412.

**IF THIS CONGRESSIONAL CORRESPONDENCE HAS BEEN MISROUTED, PLEASE NOTIFY THE OFFICE OF LEGISLATIVE AFFAIRS IMMEDIATELY.**

\_\_\_\_\_(Name)

\_\_\_\_\_(Telephone)

DEPARTMENT OF HOMELAND SECURITY

OFFICE OF LEGISLATIVE AFFAIRS  
CONGRESSIONAL ROUTING SLIP

TRACKING NO. 125620

DUE DATE: 11/12/04

DIRECTORATE/BUREAU

- BCIS
- BTS (ICE/TSA/CBP) CC:
- MANAGEMENT
- COAST GUARD
- FEMA
  
- IAIP
  
- ODP
  
- S&T
- OLA \_\_\_\_\_
- OTHER \_\_\_\_\_



*Please indicate  
urgency of  
response*

This Congressional correspondence has been forwarded to your office for a response. Please draft a response (setup for Pamela J. Turner's signature) and forward it via e-mail to [Congressionalcorrespondence@dhs.gov](mailto:Congressionalcorrespondence@dhs.gov). Also, provide a POC from your office on the lines below. If you have any questions, please contact the Office of Legislative Affairs at (202) 205-4412.

**IF THIS CONGRESSIONAL CORRESPONDENCE HAS BEEN MISROUTED, PLEASE NOTIFY THE OFFICE OF LEGISLATIVE AFFAIRS IMMEDIATELY.**

\_\_\_\_\_ (Name)

\_\_\_\_\_ (Telephone)

# Congress of the United States

Washington, DC 20515

October 26, 2004

The Honorable Tom Ridge  
Secretary  
Department of Homeland Security  
Washington, DC 20528

Dear Secretary Ridge:

We are writing to urge you to immediately require all cargo being placed on passenger airplanes to be screened for explosives in light of the recent revelation that more than 300 tons of high explosives are missing in Iraq. We are particularly concerned about cargo packages weighing less than 16 ounces, since published reports have suggested that less than 16 ounces of the type of explosives missing destroyed Pan Am Flight 103 over Lockerbie, Scotland, and since packages weighing less than 16 ounces are currently not subjected to any screening requirements whatsoever.

On October 10, 2004 Iraq's Ministry of Science and Technology officially reported that 377 tons of the explosives HMX, RDX and PETN from the site Al Qaqaa are gone and likely in the hands of terrorists<sup>1</sup>, despite IAEA warnings to the U.S. that the sites containing these materials needed to be secured. The explosives can be used to detonate nuclear bombs, but HMX and RDX are also the key components used in plastic explosives, which have been widely used in car bombings in Iraq to kill U.S. and Iraqi forces.<sup>2</sup>

Unfortunately, this is not the only situation where a well-known risk to our security from such explosives has been left unaddressed despite repeated warnings. The same explosives that disappeared from the unguarded facility in Iraq could end up in the cargo hold of a passenger plane in the United States because, as you know, with respect to the threat from packages weighing less than 16 ounces, our passenger planes are essentially unguarded.

This is a well-known threat. Plastic explosives weighing less than 16 ounces brought down Pan Am Flight 103 over Lockerbie, Scotland when terrorists planted them in unscreened baggage. We have long been concerned that packages weighing less than 16 ounces are not even subject to the inadequate known shipper program, which your Department has insisted can be securely applied to larger cargo packages in lieu of actual screening. While we continue to believe that *all* cargo should be screened for explosives, the fact that less than 1 pound of the more than 300 tons of sophisticated explosives that are missing could destroy an aircraft is particularly alarming.

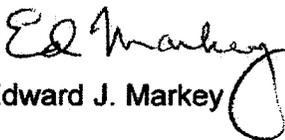
---

<sup>1</sup> "Huge cache of explosives vanished from site in Iraq," *The New York Times*, October 25, 2004.

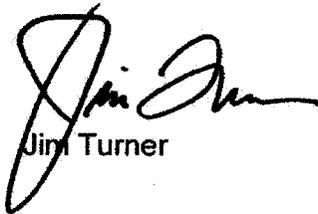
<sup>2</sup> "Tons of Iraqi explosives missing," *BBC News*, October 25, 2004.

After the tragic terrorist attack in Beslan, the Transportation Security Administration (TSA) began screening cargo placed on some passenger flights entering the U.S. from Moscow. We believe the theft of these explosives in Iraq should be treated with an even greater sense of urgency and responded to accordingly by immediately commencing the screening of all cargo being placed on passenger airlines. Failure to do so would subject millions of Americans to unnecessary risk.

Thank you very much for your attention to this important matter. Please provide your response no later than Friday October 29, 2004, and please ensure that your response includes a complete description of the steps you are taking or have already taken to close this gaping security loophole. If you have any questions or concerns, please have your staff contact Michal Freedhoff in Rep. Markey's office at 202-225-2836 or David Grannis of the Homeland Security Democratic staff at 202-226-2616.

  
Edward J. Markey

Sincerely,

  
Jim Turner

TSA 1011027015

NOV 10 2004

The Honorable Edward J. Markey  
U.S. House of Representatives  
Washington, DC 20515

Dear Congressman Markey:

Thank you for your letter to Secretary Ridge of October 26, 2004, cosigned by Congressman Jim Turner, expressing concern about the reported disappearance of explosives in Iraq, and requesting the Transportation Security Administration (TSA) to screen 100 percent of all cargo transported on passenger aircraft.

The availability of explosives throughout the world continues to be a concern for the Department of Homeland Security (DHS) and TSA. Every day TSA's Transportation Security Intelligence Service tracks and reports on existing threats and intelligence received from our intelligence community. This intelligence is used to make threat-based, risk mitigation decisions.

At this time, there is no increase in the risk posed by terrorists in using explosives in attacks against transportation, specifically aviation, assets.

As you know, TSA has been working diligently to enhance the screening of air cargo and to strengthen security across the entire supply chain. TSA's Air Cargo Strategic Plan is the cornerstone of the Department's approach to ensuring that 100 percent of cargo deemed to be of elevated risk is inspected, and to ensure that the entire air cargo supply chain is secure. To accomplish this goal, TSA has developed an automated known shipper database to verify shipper information and is developing a freight assessment system that will use analytical tools to compare shipper information with relevant threat data. The Air Cargo Strategic Plan will be supported by a notice of proposed rulemaking and accompanying security program revisions in the coming months.

In the interim, TSA continues to evaluate the applicability of current explosive detection technology in the air cargo environment by expanding the number of pilot programs being tested. TSA also continues to operationally test explosives detection canines under all conditions and deploy hundreds of inspectors focused on air cargo compliance. Over the past several months, these inspectors have begun targeted "cargo strikes" (the deployment of numerous cargo inspectors to conduct compliance inspections) at major U.S. cargo facilities.

Working closely with Congress, TSA will soon implement a provision in the FY 2005 DHS Appropriations Act (P.L. 108-334) that triples the percentage of cargo inspected by the air carriers on passenger aircraft and will expand its aggressive research and

development program by \$75 million to provide effective and efficient methods of detecting and mitigating air cargo threats (including hardened containers).

TSA's air cargo security mission is to provide the most effective security regime possible while responsibly stewarding resources and without unduly impeding the flow of commerce. TSA will continue to work closely with air cargo stakeholders, Congress, and other Federal agencies to strike this critical balance.

I appreciate your interest in the Department of Homeland Security, and look forward to working with you on future homeland security issues. An identical letter has been sent to Congressman Turner. If we may be of assistance, please contact the Office of Legislative Affairs at (202) 205-4412.

Sincerely,

Pamela J. Turner  
Assistant Secretary for Legislative Affairs

The Honorable Jim Turner  
U.S. House of Representatives  
Washington, DC 20515

Dear Congressman Turner:

Thank you for your letter to Secretary Ridge of October 26, 2004, cosigned by Congressman Edward J. Markey, expressing concern about the reported disappearance of explosives in Iraq, and requesting the Transportation Security Administration (TSA) to screen 100 percent of all cargo transported on passenger aircraft.

The availability of explosives throughout the world continues to be a concern for the Department of Homeland Security (DHS) and TSA. Every day TSA's Transportation Security Intelligence Service tracks and reports on existing threats and intelligence received from our intelligence community. This intelligence is used to make threat-based, risk mitigation decisions.

At this time, there is no increase in the risk posed by terrorists in using explosives in attacks against transportation, specifically aviation, assets.

As you know, TSA has been working diligently to enhance the screening of air cargo and to strengthen security across the entire supply chain. TSA's Air Cargo Strategic Plan is the cornerstone of the Department's approach to ensuring that 100 percent of cargo deemed to be of elevated risk is inspected, and to ensure that the entire air cargo supply chain is secure. To accomplish this goal, TSA has developed an automated known shipper database to verify shipper information and is developing a freight assessment system that will use analytical tools to compare shipper information with relevant threat data. The Air Cargo Strategic Plan will be supported by a notice of proposed rulemaking and accompanying security program revisions in the coming months.

In the interim, TSA continues to evaluate the applicability of current explosive detection technology in the air cargo environment by expanding the number of pilot programs being tested. TSA also continues to operationally test explosives detection canines under all conditions and deploy hundreds of inspectors focused on air cargo compliance. Over the past several months, these inspectors have begun targeted "cargo strikes" (the deployment of numerous cargo inspectors to conduct compliance inspections) at major U.S. cargo facilities.

Working closely with Congress, TSA will soon implement a provision in the FY 2005 DHS Appropriations Act (P.L. 108-334) that triples the percentage of cargo inspected by the air carriers on passenger aircraft and will expand its aggressive research and

development program by \$75 million to provide effective and efficient methods of detecting and mitigating air cargo threats (including hardened containers).

TSA's air cargo security mission is to provide the most effective security regime possible while responsibly stewarding resources and without unduly impeding the flow of commerce. TSA will continue to work closely with air cargo stakeholders, Congress, and other Federal agencies to strike this critical balance.

I appreciate your interest in the Department of Homeland Security, and look forward to working with you on future homeland security issues. An identical letter has been sent to Congressman Markey. If we may be of assistance, please contact the Office of Legislative Affairs at (202) 205-4412.

Sincerely,

Pamela J. Turner  
Assistant Secretary for Legislative Affairs

Simultaneous Coordination



Transportation Security Administration

# TSA CLEARANCE SHEET

ORIGINATOR  
 NOV 2 2004  
 [Redacted]  
 OFFICE: Operations Policy  
 PHONE: [Redacted]  
 DATE: 10-29-04

ns

DOCUMENT FOR ACTION  
 Action Memo     Letter  
 Info. Memo     Other

SUBJECT: Letter to Congressmen Edward J. Markey and Jim Turner who wrote to Secretary Ridge expressing concern about the reported disappearance of explosives in Iraq and requesting TSA require the screening of all cargo to be transported on passenger aircraft

TSA CONTROL NUMBER: TSA-041027-015      ACTION REQUIRED

REVIEWERS	Office	Direct Phone No.	Initial	Date	Correction Required
1.	Legal				
2.	Intel				
3.	OTSP		[Redacted]		Letter too long. Cut down to one page. red me
4.	CTO				
5.	AvOps				
6.	Ops Policy				
7.	COO				

EXECUTIVE SECRETARIAT	INITIAL	DATE	CORRECTION REQUESTED
Logging			
Review	[Signature]	10/1/04	

OFFICE OF THE ADMINISTRATOR	INITIAL	DATE	CORRECTION REQUESTED
1. Deputy Administrator	[Signature]	11/2/04	OK
2. Assistant Secretary	[Signature]	11/8	ok Done
3.			
4. [Redacted]	CSSO	11/3	Minor edits Done
5.			

Explanation, Special Instructions, Comments:



**Transportation Security Administration**

# TSA CLEARANCE SHEET

ORIGINATOR

b(6)

DOCUMENT FOR ACTION

OFFICE

PHONE

DATE

- Action Memo       Letter  
 Info. Memo       Other

Operations Policy

b(2), b(6)

10-29-04

**SUBJECT:**

Letter to Congressmen Edward J. Markey and Jim Turner who wrote to Secretary Ridge expressing concern about the reported disappearance of explosives in Iraq and requesting TSA require the screening of all cargo to be transported on passenger aircraft

TSA CONTROL NUMBER

TSA-041027-015

ACTION REQUIRED

**REVIEWERS**

#	Name	Office	Direct Phone No.	Initial	Date	Correction Required
1.	b(6)	Legal		b(6)	10-29-04	✓
2.	b(6)	Intel		b(6)	10-29-04	
3.	b(6)	OTSP		b(6)		
4.	b(6)	CTO		b(6)	10-29-04	
5.	b(6)	AvOps		b(6)	10-29-04	
6.	b(6)	Ops Policy		b(6)	10-29-04	
7.	b(6)	COO		b(6)		

**EXECUTIVE SECRETARIAT**

INITIAL

DATE

CORRECTION REQUESTED

Logging      *[Signature]*      ME      10/01/04

Review

**OFFICE OF THE ADMINISTRATOR**

INITIAL

DATE

CORRECTION REQUESTED

1.	Deputy Administrator				
2.	Assistant Secretary				
3.					
4.					
5.					

**Explanation, Special Instructions, Comments:**

148921

**Bynum, Marsha**

---

**From:** b(6)  
**Sent:** Friday, December 03, 2004 2:00 PM  
**To:** Bynum, Marsha  
**Subject:** FW: Please track

-----Original Message-----

**From:** b(6)  
**Sent:** Friday, December 03, 2004 1:49 PM  
**To:** Higgins, Patricia  
**Subject:** Please track

b(6)  
Department of Homeland Security  
Science & Technology Directorate  
Phone: b(2), b(6)  
Fax: [REDACTED]

CHRISTOPHER COOK, CALIFORNIA  
CHAIRMAN

JENNIFER DUNN, WASHINGTON  
VICE CHAIRPERSON

C. W. BILL YOUNG, FLORIDA

DON YOUNG, ALABAMA

F. JAMES SENECHERRIEMER, JR., WISCONSIN

DAVID DIERER, CALIFORNIA

LUNCAN FUNTUN, CALIFORNIA

HAROLD ROBERTS, KENTUCKY

SHERWOOD ROSENBLATT, NEW YORK

JOE BAXTON, TEXAS

LAMAR SMITH, TEXAS

CLAY WELDON, PENNSYLVANIA

CHRISTOPHER SHAYS, CONNECTICUT

PORTER J. GOSB, FLORIDA

DAVE CAMP, MICHIGAN

LINCOLN DIAZ-BALART, FLORIDA

ROBERT W. GODDOLATT, VIRGINIA

ERNEST J. STODOL, JR., OKLAHOMA

PETER T. KING, NEW YORK

JOHN LINCOLN, GEORGIA

JOHN E. SHADROG, ARIZONA

MARK SOUDER, INDIANA

MAE THORNBERY, TEXAS

JIM GIBSON, NEVADA

KAY GRANGER, TEXAS

PETE HOESONS, TEXAS

JOHN E. SHENNEY, NEW YORK

JOHN GARRISON  
Staff Director

STEPHEN DEWINE  
Deputy Staff Director and  
General Counsel

THOMAS OLENSE  
Chief Counsel and  
Policy Director



One Hundred Eighth Congress  
U.S. House of Representatives  
Select Committee on Homeland Security  
Washington, DC 20515

November 18, 2004

JOE TURNER, TEXAS

RAMON AZAROFF

BENNETT G. THOMPSON, MISSISSIPPI

LORRYTTA T. SANCHEZ, CALIFORNIA

EDWARD J. MARKEY, MASSACHUSETTS

MORRIS D. DECK, WASHINGTON

BARNEY FRANK, MASSACHUSETTS

JAMES HAYMAN, CALIFORNIA

DELLAMINI L. CARDO, MARYLAND

LOUISE M. BLANCHET, NEW YORK

PETER A. DEFAZIO, OREGON

NYTA M. LOWRY, NEW YORK

ROBERT C. ANDERSON, NEW JERSEY

ELEANOR HOLMES NORTON,  
DISTRICT OF COLUMBIA

JOE LOPEZ, CALIFORNIA

SARAH MCCARTHY, MISSOURI

SHERA JACKSON-LEE, TEXAS

BILL PASCRELL, JR., NEW JERSEY

DONNA M. CHRISTENSEN, U.S. VIRGIN ISLANDS

BOB STYERIDGE, NORTH CAROLINA

REN LUCAS, KENTUCKY

JAMES R. LANGEVIN, RHODE ISLAND

KENNEDY E. AMES, FLORIDA

BEN CHANDLER, KENTUCKY

DAVID SCHAMBER  
Deputy Staff Director and  
Chief Counsel

MARK T. MAGGE  
Deputy Chief of Staff Director

Mr. Mel Bernstein, Director  
University Programs  
Office of Research and Development  
Science and Technology Directorate  
U.S. Department of Homeland Security  
Washington, DC 20528

Dear Mr. Bernstein:

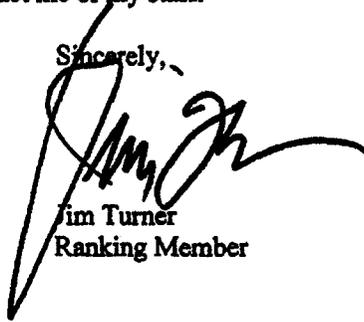
I am writing in support of a grant application submitted by Texas A&M International University in Laredo, Texas to the Homeland Security Center for Behavioral and Social Aspects of Terrorism and Counter-Terrorism.

Texas A&M International's application includes two critical projects that would help improve the ability of first responders to respond more quickly to terrorist attacks or natural disasters occurring along the U.S.-Mexico border. The first project involves developing a Geographic Information System (GIS) information database to map the location of informal rural settlements, called colonias, along the U.S.-Mexico border. This GIS database would provide first responders - and any other state or federal agencies responding to a disaster - with information about the location and critical infrastructure for each colonia. The second project would provide training in conjunction with the City of Laredo's local fire department to enhance neighborhood response capabilities in the event of a local disaster or terrorist attack.

Texas A&M International University already has an outstanding reputation in South Texas due to its advanced graduate programs and extensive ties to the community and local, state, and federal agencies. Because many of these agencies are concerned with Homeland Security, they have made their personnel and assets available for the University's Border Security Center to fulfill its mission and bolster their own performance. These two projects would expand on the assets available to the University to continue strengthening homeland security preparedness in the border region. That is why I support Texas A&M International's grant request for \$218,638 to implement the GIS database project and the community training project.

Thank you in advance for your consideration of their application. If you have any questions, please do not hesitate to contact me or my staff.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim Turner", written over the word "Sincerely,".

Jim Turner  
Ranking Member

DEC 22 2004

*Assistant Secretary for Legislative Affairs*

U.S. Department of Homeland Security

Washington, DC 20528



# Homeland Security

The Honorable Jim Turner  
U.S. House of Representatives  
Washington, DC 20515

Dear Representative Turner:

Thank you for your letter of November 18, 2004, regarding the Department of Homeland Security Centers of Excellence competition on Behavioral and Social Aspects of Terrorism and Counter-Terrorism in support of Texas A&M International University in Laredo, Texas, one of the partners in the proposal submitted by Michigan State University.

Selection of the Centers of Excellence is a highly competitive process and since the competition on this center is currently underway, this letter serves as an interim response.

The Department's Science and Technology Directorate uses a three-tiered meritorious review process to ensure the selection of the most qualified university. Following the announcement and closing of a Broad Agency Announcement, the directorate convenes a team of expert external evaluators to review all the proposals focusing on scientific merit, management, and educational outreach strategies. The most meritorious proposals are then reviewed internally by the directorate and its interagency partners for scientific merit and mission-relevancy of the specific program of work proposed. Through a site review, the directorate confirms the strengths and weaknesses found in the external and internal reviews leading to an award recommendation and ultimate selection. This review process ensures that Texas A&M and all other universities receive a fair assessment and that DHS and the nation receive the best talent and desired results.

Please be assured that upon completion of the selection process, you will receive a final reply announcing which university will house the new center.

I appreciate your interest in the Department of Homeland Security, and I look forward to working with you on future homeland security issues. If I may be of further assistance, please contact the Office of Legislative Affairs at (202) 205-4412.

Sincerely,

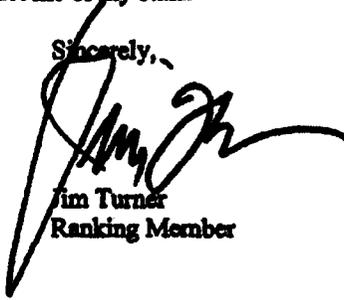
A handwritten signature in cursive script, appearing to read "Pam J.", with a long horizontal flourish extending to the right.

Pamela J. Turner  
Assistant Secretary for Legislative Affairs



Thank you in advance for your consideration of their application. If you have any questions, please do not hesitate to contact me or my staff.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim Turner", written over the word "Sincerely,".

Jim Turner  
Ranking Member

148921

**Bynum, Marsha**

---

**From:** b(6)  
**Sent:** Friday, December 03, 2004 2:00 PM  
**To:** Bynum, Marsha  
**Subject:** FW: Please track

-----Original Message-----

**From:** b(6)  
**Sent:** Friday, December 03, 2004 1:49 PM  
**To:** b(6)  
**Subject:** Please track

b(6)  
Department of Homeland Security  
Science & Technology Directorate  
Phone: b(2), b(6)  
Fax: [REDACTED]

148921

**Bynum, Marsha**

---

**From:** b(6)  
**Sent:** Friday, December 03, 2004 2:00 PM  
**To:** Bynum, Marsha  
**Subject:** FW: Please track

-----Original Message-----

**From:** b(6)  
**Sent:** Friday, December 03, 2004 1:49 PM  
**To:** Higgins, Patricia  
**Subject:** Please track

b(6)  
Department of Homeland Security  
Science & Technology Directorate  
Phone: b(2), b(6)  
Fax: b(6)

CHRISTOPHER COOK, CALIFORNIA  
CHAIRMAN

JENNIFER DUNN, WASHINGTON  
VICE CHAIRPERSON

C. W. BILL YOUNG, FLORIDA

DON YOUNG, ALABAMA

F. JAMES GERGENBRENNER, JR., WISCONSIN

DAVID DIERER, CALIFORNIA

LUNCAN FUNTUN, CALIFORNIA

HAROLD ROBERTS, KENTUCKY

SHERWOOD ROSENBLATT, NEW YORK

JOE BAXTON, TEXAS

LAMAR SMITH, TEXAS

CLAY WELDON, PENNSYLVANIA

CHRISTOPHER SHAYS, CONNECTICUT

PORTER J. GOSB, FLORIDA

DAVE CAMP, MICHIGAN

LINCOLN DIAZ-BALART, FLORIDA

ROBERT W. GODDOLATT, VIRGINIA

ERNEST J. STODOL, JR., OKLAHOMA

PETER T. KING, NEW YORK

JOHN LINCOLN, GEORGIA

JOHN E. SHADROG, ARIZONA

MARK SOUDER, INDIANA

MAE THORNBERY, TEXAS

JIM GIBSON, NEVADA

KAY GRANGER, TEXAS

PETE HOESONS, TEXAS

JOHN E. SHENNEY, NEW YORK

JOHN GARRISON  
Staff Director

STEPHEN DEWINE  
Deputy Staff Director and  
General Counsel

THOMAS OLENSE  
Chief Counsel and  
Policy Director



One Hundred Eighth Congress  
U.S. House of Representatives  
Select Committee on Homeland Security  
Washington, DC 20515

November 18, 2004

JOE TURNER, TEXAS

RANDY AZAROFF

BENNETT G. THOMPSON, MISSISSIPPI

LORRYTTA T. SANCHEZ, CALIFORNIA

EDWARD J. MARKEY, MASSACHUSETTS

MORRIS D. DECK, WASHINGTON

BARNEY FRANK, MASSACHUSETTS

JAMES HAYMAN, CALIFORNIA

DELLAMINI L. CARDO, MARYLAND

LOUISE M. BLAUGHTER, NEW YORK

PETER A. DEFAZIO, OREGON

NYTA M. LOWMY, NEW YORK

ROBERT C. ANDERSON, NEW JERSEY

ELEANOR HOLMES NORTON,  
DISTRICT OF COLUMBIA

JOE LOPEZ, CALIFORNIA

SARAH MCCARTHY, MISSOURI

SHERA JACKSON-LEE, TEXAS

BILL PASCRELL, JR., NEW JERSEY

DONNA M. CHRISTENSEN, U.S. VIRGIN ISLANDS

BOB STYERIDGE, NORTH CAROLINA

REN LUCAS, KENTUCKY

JAMES R. LANGEVIN, RHODE ISLAND

KENNEDY E. AMES, FLORIDA

BEN CHANDLER, KENTUCKY

DAVID SCHAMBER  
Deputy Staff Director and  
Chief Counsel

MARK T. MAGGE  
Deputy Chief of Staff Director

Mr. Mel Bernstein, Director  
University Programs  
Office of Research and Development  
Science and Technology Directorate  
U.S. Department of Homeland Security  
Washington, DC 20528

Dear Mr. Bernstein:

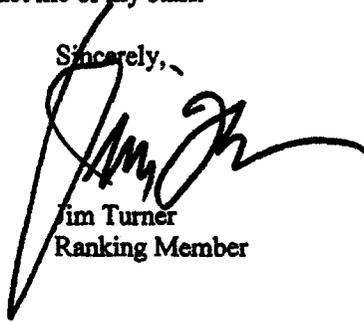
I am writing in support of a grant application submitted by Texas A&M International University in Laredo, Texas to the Homeland Security Center for Behavioral and Social Aspects of Terrorism and Counter-Terrorism.

Texas A&M International's application includes two critical projects that would help improve the ability of first responders to respond more quickly to terrorist attacks or natural disasters occurring along the U.S.-Mexico border. The first project involves developing a Geographic Information System (GIS) information database to map the location of informal rural settlements, called colonias, along the U.S.-Mexico border. This GIS database would provide first responders - and any other state or federal agencies responding to a disaster - with information about the location and critical infrastructure for each colonia. The second project would provide training in conjunction with the City of Laredo's local fire department to enhance neighborhood response capabilities in the event of a local disaster or terrorist attack.

Texas A&M International University already has an outstanding reputation in South Texas due to its advanced graduate programs and extensive ties to the community and local, state, and federal agencies. Because many of these agencies are concerned with Homeland Security, they have made their personnel and assets available for the University's Border Security Center to fulfill its mission and bolster their own performance. These two projects would expand on the assets available to the University to continue strengthening homeland security preparedness in the border region. That is why I support Texas A&M International's grant request for \$218,638 to implement the GIS database project and the community training project.

Thank you in advance for your consideration of their application. If you have any questions, please do not hesitate to contact me or my staff.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim Turner", written over the word "Sincerely,".

Jim Turner  
Ranking Member