



Privacy Impact Assessment  
for the

# USCIS International Visa Project

**DHS/USCIS/PIA-048**

**July 22, 2013**

**Contact Point**

**Donald K. Hawkins**

**Privacy Officer**

**U.S. Citizenship and Immigration Services**

**(202) 272-8030**

**Reviewing Official**

**Jonathan R. Cantor**

**Acting Chief Privacy Officer**

**Department of Homeland Security**

**(202) 343-1717**



## Abstract

Many countries now require biometric data from individuals filing applications for a visa. Several international allies have partnered with the Department of Homeland Security (DHS) U.S. Citizenship and Immigration Services (USCIS) to collect the requisite biometrics and limited biographical information on behalf of their countries. USCIS will collect biometric and biographical information and delete the records immediately after it receives confirmation that the partnering country has received the information. USCIS is conducting this Privacy Impact Assessment (PIA) to discuss the privacy risks and mitigations associated with processing information on behalf of another country.

## Overview

On March 1, 2003, the United States Citizenship and Immigration Services (USCIS) officially assumed responsibility for the immigration service functions of the U.S. Federal Government. The Homeland Security Act of 2002 (Pub. L. No. 107-296, 116 Stat. 2135) dismantled the former Immigration and Naturalization Service (INS) and separated the former agency into three components within the Department of Homeland Security (DHS).<sup>1</sup> USCIS was formed to enhance the security and improve the efficiency of national immigration services by exclusively focusing on the administration of benefit applications to immigrants and/or nonimmigrants for various reasons, such as: to work in the U.S., to bring family to the U.S., to become a permanent resident, and to become a U.S. citizen. Once an applicant submits his or her benefit application, USCIS conducts background and security checks and reviews the evidence an applicant submits to support his or her eligibility for the benefit. The background and security checks identify individuals who are improperly or fraudulently seeking immigration benefits to assist in ensuring the integrity of the U.S. immigration system.<sup>2</sup>

As part of the background and security check, USCIS requires applicants and petitioners, for certain immigration benefits, to provide their fingerprints and have their photograph taken. After an individual submits a benefit application, he or she will go to the local USCIS Applicant Support Center (ASC) for a biometrics services appointment to fulfill this requirement. At this appointment, ASC personnel capture the individual's biometrics and limited biographic information to assist in the approval or denial of the benefit application.

Similar to the U.S. immigration process, several countries have enacted legislation that requires individuals filing visa applications to submit biometric data; this increases the security of the international visa issuance process.<sup>3</sup> Some countries have begun to implement this requirement for applicants who are presently in their country and want to apply for a visa. However, individuals who need to apply for a visa are often out of the country. To assist those individuals located in the U.S., many countries have

---

<sup>1</sup> Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP), components within DHS, now handle immigration enforcement and border security functions.

<sup>2</sup> In the past, these security checks have yielded information about applicants involved in serious crimes, including crimes against children, drug trafficking, and applicants with known links to terrorism.

<sup>3</sup> A visa allows an individual to travel to a port of entry, airport, or land border crossing, and to request permission to the respective country's inspector to enter the country. While having a visa does not guarantee entry to the country, it does indicate that an individual is eligible to seek entry to the country for a stated purpose (e.g., business, school, pleasure).



locations in the U.S. to process applications. Unfortunately, these are only in selected locations throughout the U.S., and are generally located in coastal or metropolitan areas.

To support this process with select international allies, USCIS is expanding its biometric collection process to support the adjudication of visas for foreign countries. USCIS is offering a fee-based service to international partners to collect biometric and biographic information from individuals who are filing international visa applications who are physically present in the U.S. This service is authorized by Section 573 of the Foreign Assistance Act of 1961, (22 U.S.C. § 2349aa), which allows U.S. agencies to furnish services to foreign countries.<sup>4</sup> USCIS will provide this service to foreign partners, hereinafter referred to as partnering countries, for a fee agreed upon by each agency and set forth in a Memorandum of Understanding (MOU).

USCIS has the technology and capability to collect biometric and biographic information from a large number of people across the U.S.; there are over 130 USCIS ASCs throughout the U.S. and its territories that are equipped to collect this information. As such, USCIS is able to provide a much faster and lower cost service to the applicant. Without this service, applicants may have to travel as far as several states away to provide their biometrics. Additionally, the submission of biometrics by more countries for visa, border, and national identity schemes represents an opportunity for DHS to collaborate with partnering countries. This will allow USCIS and the partnering countries, to leverage scarce resources, influence technological innovation, and identify greater opportunities for sharing critical identity information in the future.

USCIS' successful collaboration with the United Kingdom (U.K.) since Fiscal Year 2008 demonstrates the success of this effort and suggests this service can assist other countries as well.<sup>5</sup> The use of USCIS ASCs enables partnering countries to achieve a low cost, fast, effective, and comprehensive biometrically-enabled visa system, helping to create a secure border and reduce fraud. Appendices to this PIA include a detailed description of the U.K. partnership and all other international partnerships that are currently in place.<sup>6</sup>

### *USCIS Collection of Information*

The process begins when an individual seeking an international visa completes the applicable partnering country's visa application, and submits the associated fee. After submitting the application online, the partnering country's website directs the applicant to its online scheduling system to make a biometric appointment at a USCIS ASC. The scheduling system provides the applicant with available timeslots at surrounding ASCs and instructs him or her to print an appointment letter. The partnering country uses these timeslots to assign them to the applicants to come in for an appointment. The individual will print the appointment letter and is instructed to bring the letter to the ASC.

The individual will arrive at the ASC with the appointment letter and other necessary materials (e.g., photo identification and/or travel document), depending on instructions from partnering country. ASC personnel will check the individual's photo identification and appointment letter and validate the

---

<sup>4</sup> The Foreign Assistance Act of 1961, as amended, can be found here: <http://transition.usaid.gov/policy/ads/faa.pdf>

<sup>5</sup> The U.K. was the first country to partner with the USCIS for this project.

<sup>6</sup> This PIA will supersede the previously published DHS/USCIS/PIA-011 - DHS/UKvisas Project, dated November 14, 2007.



appointment against an appointment manifest that the partnering country previously provides to the ASC, typically 48 hours in advance.

ASC personnel will collect the applicant's biographic information<sup>7</sup> (e.g., full name, date of birth, country of birth, sex, and nationality) from the appointment letter and/or photo identification and capture the individual's biometrics (i.e., fingerprints and photographs). USCIS captures fingerprints using an electronic live scan device, also referred to as an electronic fingerprint machine, that captures a print of all 10-digits.<sup>8</sup> After all information is captured, ASC personnel complete a final quality assurance review to ensure all relevant information, specific to the partnering country, is captured. ASC personnel stamp the individual's appointment letter for proof that he or she submitted biometrics to USCIS. The ASC will transmit the information to the partnering country through the USCIS Enterprise Service Bus (ESB), unless noted differently in a specific partnering country's appendix to this PIA.<sup>9</sup>

### *Transmission*

The transmission of biometric information occurs through the ESB immediately after USCIS ASC personnel capture the biometrics. USCIS will temporarily retain biographical information and biometrics captured on the ESB pending notice of successful transmission to the partnering country. USCIS will delete the information after the partnering country confirms receipt of the information and will not have the ability to retrieve any personally identifiable information (PII) associated with the visa applicant after the confirmation of the successful transfer from the partnering country. USCIS anticipates the retention period for this information to be less than 30 minutes and no longer than 12 hours.

In the rare event that the partnering country does not confirm receipt of the information, USCIS must determine why the information is not transmitting. USCIS has the capability to retrieve the information that is queued up awaiting transmission to determine if the problem is equipment or transmission-related. USCIS can do this by using a combination of the country code and random numbers that enables locating and tracking the case. Once USCIS identifies the problem, ASC personnel either resend the information to the partnering country, or may require the applicant to come in for another biometric appointment.

To account for the transmission, USCIS retains an audit log that includes a transaction control number,<sup>10</sup> date and time of transaction, machine identification number, and employee identification number. This data is separate from, and cannot be linked to, the PII described above, and is retained by the USCIS enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR). eCISCOR provides backup information in support of billing and monthly reporting to be sent to the partnering country.<sup>11</sup> USCIS will advise the respective partnering country that the audit logs were deleted after they are no longer needed.

---

<sup>7</sup> The biographic information collected may vary by country; please see the appendices to this PIA for complete details.

<sup>8</sup> Ordinarily, all ten fingerprints will be captured in this process; however, if one or more fingers are not available (for instance, because of amputation) then USCIS will capture as many fingers as are available.

<sup>9</sup> The DHS/USCIS/PIA-008 - Enterprise Service Bus (ESB) PIA can be found at [www.dhs.gov](http://www.dhs.gov).

<sup>10</sup> This is a combination of a country code and numbers that is unique to each country.

<sup>11</sup> The DHS/USCIS/PIA-023-eCISCOR can be found at [www.dhs.gov](http://www.dhs.gov).



## *Authentication*

While USCIS ASCs will perform a preliminary check to confirm an individual's identity, USCIS is not responsible for officially authenticating an individual's identity on behalf of the partnering country. ASC personnel will only check the individual's photo identification and validate the appointment against the appointment manifest that the partnering country provides.

Upon receiving the biometric information from USCIS, the partnering country will use the biometric information in support of its decision to grant or deny a visa. The process each partnering country follows is in accordance with its respective policies and Standard Operating Procedures.

Additionally, the official authentication of an individual occurs when an individual enters the foreign country. When the individual arrives in the country, an immigration officer will greet him or her and ask to see photo identification, travel documents, and any other relevant information for verification purposes. The partnering country's immigration officers perform the ultimate authentication of an individual's identity at the time of entry into the country. The officer will verify the documentation and ask the individual questions to determine if they meet the requirements for admission into the country. The officer will officially determine if the individual is authorized to enter the country.

## *DHS Sharing*

After USCIS transmits the data to the partnering country, that country may transfer the biometric and biographic information to the DHS Office of Biometric Identity Management (OBIM, formerly US-VISIT) for further analysis. USCIS does not share the visa information associated with this project with OBIM. USCIS sends the data associated with this project directly to the partner country, and the country may elect to enter a separate sharing agreement with OBIM. These sharing arrangements vary by country and are governed by separate information sharing access agreements.

If a country chooses to forward the biometric and biographic information collected by USCIS to OBIM, OBIM will query the biometric information against the Automated Biometric Identification System's (IDENT)<sup>12</sup> list of subjects of interest (e.g., "Subjects of interest" are people of interest to the U.S. or international law enforcement and/or intelligence agencies because of suspected or confirmed illegal activity). OBIM will provide the country with results from the query, along with, in some cases, details of the analysis supporting the returned results. This assists the partnering country in its determination of whether visa applicants are eligible to obtain visas or other travel documents according to its applicable laws.

Any partnering country using the OBIM service will have a separate MOU in place regarding the specifics of that sharing agreement. The IDENT PIA will also include information on each country's agreement in its appendix.

---

<sup>12</sup> The DHS/NPPD/USVISIT/PIA-002 IDENT PIA can be found at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).



## Section 1.0 Authorities and Other Requirements

### 1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Section 573 of the Foreign Assistance Act of 1961, (22 U.S.C. § 2349aa), authorizes USCIS to conduct this fee-based service for international agencies. In addition, DHS has signed a MOU with each partnering country that uses USCIS ASCs for this service. Each MOU defines the technical roles, responsibilities, and processes of USCIS and the partnering country.

### 1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

USCIS is temporarily retaining information collected on behalf of its partnering country and does not retrieve the records using a unique personal identifier. The biographical information and biometric capture is transferred to the partnering country immediately after collection. USCIS will delete the information from the ESB after the partnering country provides confirmation of the successful transfer of the information. Therefore, no SORN is required to cover this PIA.

### 1.3 Has a system security plan been completed for the information system(s) supporting the project?

ESB is the information technology system that supports the temporary storage and onward transfer of information to the partnering country. ESB was authorized for operation on July 1, 2013, for a period of 12 months. The ESB Authority to Operate (ATO) is set to expire on July 1, 2014. The ESB Security Plan was completed on September 8, 2011.

eCISCOR is the system supporting the storage of the audit information. eCISCOR's ATO began on December 19, 2012, for a period of 18 months. The eCISCOR ATO expires on June 19, 2014. The eCISCOR Security Plan was completed on September 18, 2012.

### 1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

USCIS does not retain international visa applicant information beyond the point at which it has received confirmation that the partnering country has received the information. USCIS anticipates the retention period will routinely be less than 30 minutes and no longer than 12 hours. Because USCIS is retaining these records for such a short period of time, no retention schedule is needed for the international visa applicant information.

USCIS will retain audit logs of these transactions within eCISCOR. This information is available online for a period of 180 days. Offsite retention of this information is for seven years. This requirement is per *Section 5.3 - Audit Logs Maintained* of the DHS - 4300A, which states, "Audit trail records must be maintained online for at least 90 days, thereby allowing rapid access to recent information. Audit trails



should be preserved for a period of seven years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease.” This is the standard retention period specified by DHS Security Authorization policy for system audit data; therefore, no NARA retention schedule exists.

## **1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.**

The Paperwork Reduction Act is a requirement that must be fulfilled by the U.S. Federal government. The service described in this PIA uses applications and forms furnished by international agencies, which are not obligated to follow the Paperwork Reduction Act.

## **Section 2.0 Characterization of the Information**

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

### **2.1 Identify the information the project collects, uses, disseminates, or maintains.**

The USCIS international visa project collects biographic and captures biometric information from individuals applying for a visa in another country. This project collects information from individuals who are physically present in the U.S. (e.g., U.S. Lawful Permanent Residents, third country nationals, and U.S. Citizens) who require a visa to travel to a particular country.

The information that USCIS obtains from individuals to assist in processing international visa applications includes biographic and biometric data. The biometric information includes 10-print fingerprints captured by the electronic live scan device and photographs. The biographic data may include, but is not limited to, first and last name; date of birth; country of birth; sex; and nationality. These data elements will be assembled into a secure format for transmission from the ASC to the partnering country.

### **2.2 What are the sources of the information and how is the information collected for the project?**

USCIS obtains information it collects directly from individuals who are applying for international visas and are physically present in the U.S. at the time of biometric capture. Fingerprints and photos are captured electronically at one of USCIS’ ASCs, while biographic information is provided by the applicant through the appointment letter generated by the foreign country’s application system. Visa applicants include third country nationals, Lawful Permanent Residents, and U.S. citizens.



### **2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.**

USCIS does not collect information from commercial or publicly available data sources to for the purposes of this project.

### **2.4 Discuss how accuracy of the data is ensured.**

The information USCIS collects and transfers to the partnering country is assumed to be accurate, because it is collected directly from the individual applying for an international visa. ASC personnel verify that the photographs and fingerprints they collect are clear and usable before transferring the information to the partnering country.

### **2.5 Privacy Impact Analysis: Related to Characterization of the Information**

**Privacy Risk:** There is a risk that the information sent to the partnering country may be inaccurate.

**Mitigation:** All information that USCIS provides to the partnering country is collected directly from the individual applying for an international visa. USCIS personnel will compare the identity of the individual present for a biometric appointment against information provided by the international office on the applicant appointment letter. If USCIS determines the individual is the person applying for a visa, USCIS will collect limited biographic information from the appointment letter and biometric information and send it to the partnering country. Once the partnering country receives the information from USCIS, it is the responsibility of the partnering country to confirm the accuracy of the data and to determine if the individual is eligible to receive a visa.

## **Section 3.0 Uses of the Information**

The following questions require a clear description of the project's use of information.

### **3.1 Describe how and why the project uses the information.**

USCIS does not use the information collected as part of this program. USCIS serves only as the front-end data gathering agent for the partnering country. USCIS will transfer the information to the partner country to use during the review of the application for that country to ultimately grant or deny a visa to the applicant. Appendices to this PIA include a detailed description of how each country uses the biometric information.

After confirmation of receipt by the visa issuing office, the information is deleted from the USCIS ESB and cannot be used or retrieved by USCIS.



### **3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.**

USCIS does not use technology to conduct pattern based queries or searches for the purposes of this project.

### **3.3 Are there other components with assigned roles and responsibilities within the system?**

USCIS does not share this information with organizations internal to DHS. Participating partnering countries may opt to share data collected as part of this program with DHS OBIM, but USCIS only sends the collected biographic and biometric information back to the partnering country.

### **3.4 Privacy Impact Analysis: Related to the Uses of Information**

**Privacy Risk:** There is a risk that the information collected may be used for purposes other than sending the data to the partnering country.

**Mitigation:** This risk is mitigated by USCIS only temporarily retaining the information collected on behalf of the partnering country. USCIS collects this information, temporarily stores it on the USCIS ESB, transfers it to the partnering country, and then purges it once USCIS confirms the partnering country has received the data. Because USCIS does not retain this information and it is not retrievable in the future, USCIS cannot use the data for any reason other than the stated purpose.

## **Section 4.0 Notice**

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

### **4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.**

Individuals receive notice of the biometric capture requirement during the initial international visa application process. When individuals submit their visa application to the partnering country, they are immediately notified to make a biometric appointment with USCIS as part of the application process. Detailed instructions are provided through the partnering country's application system regarding the closest ASC for processing, when to arrive, what to bring, and additional details pertaining to the appointment. A summary of this information is included in the appointment letter.

Additionally, notice of the collection is provided through this PIA. Additional notice may be provided by the partnering country.



## 4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals who apply for international visas are required to submit their biometrics and limited biographical information. However, the partnering country, not the U.S. government, may determine if an individual has an opportunity to decline to provide the information.

Additionally, the use of a USCIS ASC is voluntary. An international visa applicant may choose to submit his or her application and biometrics using another approved method. The applicant should contact the partnering country for other options.

## 4.3 Privacy Impact Analysis: Related to Notice

**Privacy Risk:** There is a risk that USCIS and the partnering country may provide insufficient notice to the individual of the purpose and use of his or her information.

**Mitigation:** USCIS mitigates this risk by providing notice to the individual through the publication of this PIA, public outreach efforts, and information on [www.uscis.gov](http://www.uscis.gov). Additionally, each partnering country publishes its visa application requirements on its website to inform applicants, and provides additional notice on this program in the appointment letter. Appendices to this PIA discuss specific notice provided by each partnering country.

## Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

### 5.1 Explain how long and for what reason the information is retained.

USCIS will not retain information beyond the point at which USCIS has received confirmation that the partnering country has received the information. USCIS anticipates that the retention period will routinely be less than 30 minutes and no longer than 12 hours. Because USCIS will only retain these records for such a short period of time, no retention schedule is needed for the international applicant data.

USCIS will retain audit logs of these transactions within ESB. This data is available online for a period of 180 days. Offsite retention of this data is for seven years. This requirement is per *Section 5.3 - Audit Logs Maintained* of the DHS - 4300A, which states, "Audit trail records must be maintained online for at least 90 days, thereby allowing rapid access to recent information. Audit trails should be preserved for a period of seven years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease." This is the standard retention period specified by DHS Certification and Accreditation (C&A) policy for system audit data; therefore, no NARA retention schedule exists.



## 5.2 Privacy Impact Analysis: Related to Retention

**Privacy Risk:** There is a risk that USCIS is collecting and retaining information that is not related to the USCIS mission.

**Mitigation:** USCIS is assisting partnering countries by collecting information that is needed to adjudicate foreign visas, pursuant to Section 573 of the Foreign Assistance Act of 1961, (22 U.S.C. § 2349aa). USCIS collects the information on behalf of the partnering country and sends the information directly to the country. USCIS retains the information for the brief time to ensure a successful transfer to the partnering country. If a failure in the transmission occurs, the brief retention period will afford USCIS the ability to resend the record to make sure the information is successfully transferred to the international office. Once USCIS receives confirmation that the transfer of data was successful; the biometric records are deleted from USCIS ESB.

## Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

### 6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

USCIS has signed MOUs in place with each partnering country. See appendices to this PIA for details. Appendices will be added as USCIS enters into additional MOUs.

### 6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

No SORN is required for this external sharing because USCIS deletes the data immediately after the international office confirms it has received the transfer.

### 6.3 Does the project place limitations on re-dissemination?

All of the MOUs that are currently in place discuss limitations on re-dissemination. Appendices to this PIA will discuss these limitations with USCIS' external partners.

### 6.4 Describe how the project maintains a record of any disclosures outside of the Department.

This project maintains records of disclosures through audit logs. The audit logs include a unique transaction control number, date and time of transaction, machine identification number, and employee identification number. This data is separate from, and cannot be tied to, the PII described above. USCIS retains this data for billing purposes.



## 6.5 Privacy Impact Analysis: Related to Information Sharing

**Privacy Risk:** There is a privacy risk of unauthorized disclosure.

**Mitigation:** Because USCIS only retains the information for a short period of time, the risk of unauthorized disclosure is very limited. However, this risk is still mitigated in a number of ways. First, all external partners are required to sign information sharing agreements or MOUs. These documents outline the limitations on dissemination and the steps needed in order for parties to appropriately disseminate information outside of the Department, if applicable. Additionally, all users that handle the data associated with this project must conform to appropriate security and privacy policies, follow established rules of behavior, and receive training regarding the security of DHS systems.

## Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

### 7.1 **What are the procedures that allow individuals to access their information?**

There is no long-term retention of records associated with this project. USCIS is capturing and transmitting the information on behalf of the partnering country. USCIS does not provide redress to foreign country visa applicants. Because USCIS does not retrieve the information by personal identifier and it is purged after the partnering country confirms the receipt of the information, USCIS cannot provide the applicant with access to his or her requested information. Therefore, USCIS recommends contacting the respective partnering country directly. Appendices to this PIA will discuss these procedures.

### 7.2 **What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?**

See the appendices to this PIA for a detailed description of the respective partnering country's redress policies.

### 7.3 **How does the project notify individuals about the procedures for correcting their information?**

See the appendices to this PIA for a detailed description of each partnering country's redress policies.

## 7.4 Privacy Impact Analysis: Related to Redress

**Privacy Risk:** USCIS does not provide redress to individuals who apply for foreign country visas.



**Mitigation:** USCIS provides a service to partnering countries. USCIS collects the information on behalf of the partnering country and only temporarily stores the information that is sent to the country. Therefore, USCIS does not provide redress to visa applicants for foreign countries. This risk is mitigated by having each international office provide its own form of redress to applicants.

## Section 8.0 Auditing and Accountability

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

### **8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?**

DHS security specifications require auditing capabilities that log the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. In accordance with DHS security guidelines, USCIS systems use auditing capabilities that log user activity. All user actions are tracked via audit logs to identify audit information by employee identification number, date, and time of transaction. These audit logs are also maintained to keep track of monthly billing and reporting inquiries to each country.

### **8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.**

USCIS provides annual privacy and security awareness training to all employees and contractors. The Culture of Privacy Awareness training addresses appropriate privacy concerns, including Privacy Act obligations (e.g., SORNs and Privacy Act Statements). The Computer Security Awareness training examines appropriate technical, physical, personnel, and administrative controls to safeguard information. Additionally, all employees employed by the receiving agency are given specific training on how to safeguard applicant data.

### **8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?**

Only USCIS ASC personnel with a valid need-to-know will have access to the information they collect as part of this project. All ASC personnel who collect information as part of this project have security clearances that are documented by the USCIS Office of Security and the ASC Program Office. Additionally, the comprehensive ASC Standard Operating Procedures outline in detail who has access to biometric collection devices.



## **8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?**

USCIS has a formal review and approval process in place for new sharing agreements. Any new sharing agreements, use of information, and/or new access requests for USCIS systems must go through the USCIS change control process and must be approved by the proper authorities prior to sharing information within and outside of DHS.

### **Responsible Officials**

Donald K. Hawkins  
Privacy Officer  
U.S. Citizenship and Immigration Services  
(202) 272-8030

### **Approval Signature**

Original signed and on file at the DHS Privacy Office.

---

Jonathan R. Cantor  
Acting Chief Privacy Officer  
Department of Homeland Security



## Appendix A:

### United Kingdom (U.K) Border Agency (UKBA) International Group Visas Services Project (formerly known as UKvisas)<sup>13</sup>

#### Purpose and Use:

USCIS ASCs will collect applicant biometric and biographic information on behalf of the UKBA. UKBA will use this information to determine whether visa applicants for entry to the United Kingdom are eligible to obtain visas or other travel documents according to applicable U.K. laws.

#### MOU:

An MOU was signed on November 16, 2007, between the Director of Network Operations, UKBA (referred to as UKvisas in MOU), and the Director, U.S. Citizenship and Immigration Services.

#### Data Elements:

Applicants submit their biographic information via their visa application. USCIS ASC personnel collect the biometric data. Through this project, the following categories of information are collected:

Limited biographic information: full name, date of birth, country of birth, sex, and nationality;

Biometrics: 10 fingerprints and a photograph.

#### Transmission:

The transmission of biometric information to the UKBA occurs immediately after USCIS ASC personnel capture the biometrics through the secure electronic method. The ASC will transmit the information to the respective visa issuing country through the USCIS Biometric Storage System (BSS) in an Electronic Fingerprint Transmission Specification (EFTS), a National Institute of Standards and Technology (NIST) standard file.<sup>14</sup> USCIS plans to change the transmission through the USCIS ESB in the future. When this occurs, USCIS will update and republish this Appendix.

Messaging protocol – SMTP

Transport – VPN tunnel

Physical Network – Internet

#### Additional Sharing:

UKBA has a separate agreement in place with US-VISIT to share biometric and biographic data for identifying derogatory information.

#### Notice:

UKBA's website makes full disclosure of the need to provide biometrics for processing an application. UKBA also provides notice to the applicant to appear at an ASC for biometrics collection in the UKBA appointment letter. UKBA has also developed a handout containing additional information for

---

<sup>13</sup> The process discussed in this PIA and appendix replaces the previously published DHS/USCIS/PIA-011 - DHS / UKvisas Project, dated November 14, 2007.

<sup>14</sup> The DHS/USCIS/PIA-005 BSS PIA is available at [www.dhs.gov](http://www.dhs.gov).



applicants, which is available on its website at:

<http://www.ukba.homeoffice.gov.uk/countries/usa/applying/biometric/?langname=null>

### **Correction and Redress:**

The UKBA International Group Visa Services Project is solely responsible for granting or denying UKBA International Group Visa Services Project applications. The UKBA International Group Visa Services Project will determine whether any change to an applicant's information by USCIS, as a result of a successful redress request, will impact the adjudication process of the UKBA International Group Visa Services Project. The appeals process for handling inaccurate or erroneous information on behalf of the UKBA International Group Visa Services Project is solely the responsibility of the United Kingdom and is available on the UKBA website at [www.ukvisas.gov.uk](http://www.ukvisas.gov.uk).

If UKBA denies the applicant a visa to enter the United Kingdom, they will provide a letter of visa denial and visa appeal to the applicant. The appeals process of the UKBA International Group Visa Services Project varies based on the circumstances of the denial. The denial letter will detail the process the applicant must follow to appeal the visa decision. If UKBA denies an applicant a visa to enter the United Kingdom, the applicant may refer to the UKBA website at:

<http://www.ukba.homeoffice.gov.uk/visas-immigration/visiting/general/appeals/>.



## **Appendix B: Citizenship and Immigration Canada (CIC)**

### **Purpose and Use:**

USCIS ASCs will collect applicant biometric and biographic information on behalf of the CIC. CIC will use this information to determine whether visa applicants for entry to Canada are eligible to obtain visas or other travel documents according to applicable Canadian laws.

### **MOU:**

An MOU was signed on September 16, 2012, between the Deputy Minister of Citizenship and Immigration Canada, and the Director of U.S. Citizenship and Immigration Services.

### **Data Elements:**

Applicants submit their biographic information via their visa application. USCIS ASC personnel collect the biometric data. Through this project, the following categories of information are collected:

Limited biographic information: full name, date of birth, country of birth, sex, and nationality;

Biometrics: 10 fingerprints and a photograph.

### **Transmission:**

The transmission of biometric information to the CIC occurs immediately after USCIS ASC personnel capture the biometrics through the secure electronic method. The ASC will transmit the information to the respective visa issuing country through the USCIS ESB in an Electronic Fingerprint Transmission Specification (EFTS), a National Institute of Standards and Technology (NIST) standard file.

Data encoding – MIME attachment

Messaging protocol – SMTP

Transport – VPN tunnel

Physical Network – Internet

### **Additional Sharing:**

Currently, CIC does not have an agreement in place for sharing data with a third party. In the future, if CIC agrees to share information to third parties, USCIS will update and republish this PIA Appendix.

### **Notice:**

CIC's website makes full disclosure of the need to provide biometrics for processing an application at <http://www.cic.gc.ca/english/visit/biometrics.asp>. CIS provides notice to appear at an ASC for biometrics collection in the CIC's appointment letter.



## **Correction and Redress:**

The CIC is solely responsible for granting or denying CIC applications. The CIC will determine whether any change to an applicant's information by USCIS, as a result of a successful redress request, will impact the adjudication process of the CIC. The appeals process for handling inaccurate or erroneous information on behalf of the CIC is solely the responsibility of Canada and is available on the CIC website at <http://www.cic.gc.ca/>.

If the CIC denies the applicant a visa to enter Canada, they will provide a letter of visa denial and visa appeal to the applicant. The appeals process of the CIC varies based on the circumstances of the denial. The denial letter will detail the process the applicant must follow to appeal the visa decision. If CIC denies an applicant a visa to enter Canada, the applicant may refer to the CIC website at <http://www.cic.gc.ca/> for more information.