Privacy Impact Assessment
for the

DHS / UKvisas Project

November 14, 2007

Contact Point
Elizabeth Gaffin
Associate Counsel
United States Citizenship and Immigration Services
202-272-1400

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

Recently the United Kingdom (UK) enacted legislation requiring the submission of biometric data by almost all individuals filing applications for UK visas. Officials from the UK and Department of Homeland Security (DHS) have agreed that individuals who are physically located in the United States (US) may provide the requisite biometrics and limited biographical information at U.S. Citizenship and Immigration Services (USCIS) Application Support Centers (ASCs) for forward transfer to the UK in support of the adjudication of applications for visas. USCIS will temporarily retain the submitted biometric and biographical records until the UK provides confirmation that the transfer of data was successful. USCIS will delete the biometric and biographical records immediately after it receives that confirmation.

Introduction

UKvisas Biometric Capture Program (BCP), the UK governmental entity responsible for the granting of visas, initiated a biometric capture program in April 2005 in order to increase the security of their visa issuance process. The aim of the program is to introduce digital fingerprinting and photographic capabilities into the existing UK visa application process by 2008. The UK Program vision is to achieve a fast, effective and comprehensive biometrically enabled visa system, helping to create a secure and integrated border control. Towards that end, the UK announced that all applicants, with few exceptions (Heads of State for example), will be required to supply 10 digit fingerscans and a digital photograph when applying for a UK visa. This new procedure is supported by the UK's Article 3 of The Immigration (Provision of Physical Data) Regulations 2006. The UK has already begun collecting biometrics on visa applicants from several countries and will extend this requirement to people residing in the US by December 2007. The UK has a large volume of applications in the US but few locations in which to process them.

As part of this new requirement, UKvisas BCP has reached out to its international partners and allies to determine whether it can leverage existing processes in certain countries to capture the biometrics. UKvisas BCP and DHS conducted a viability study and determined that DHS could offer the services of the USCIS Application Support Centers (ASC) for the biometrics collection of individuals filing UK visa applications and who are physically present in the United States. The ASCs are a network of 129 geographically dispersed locations in all 50 US states and Puerto Rico, St. Thomas, Guam, and St. Croix managed by the DHS Citizenship and Immigration Service (USCIS). The ASCs were initially established to assist legacy U.S. Immigration and Naturalization Service (now part of USCIS) to collect biometric data.

An applicant for a UK visa begins the application process by completing the UK visa application, and submitting the application fee, on-line at www.visa4uk.gov.uk. The applicant will be directed by the UK to an on-line scheduling system to make an appointment for biometrics capture at a DHS ASC (or, alternatively, at the appropriate UK consulate if the applicant chooses not to submit his or her information at an ASC). The applicant will print the appointment receipt and will be instructed to bring the receipt with them to the ASC. The applicant will arrive at the ASC with their appointment receipt and photo identification (preferably a passport.) The ASC personnel will check the applicant's photo identification and validate the applicant's appointment against an appointment manifest that will be provided by UKvisas. A UK visa Entry Clearance Officer will perform the ultimate authentication of an applicant's identity at the time of entry into the UK. ASC personnel will not be required to confirm the identity of the UK visa applicant on behalf of the UK government.

All information related to the UK biometrics process will be immediately transmitted to the UK utilizing secure electronic transfer methods. These individual transmissions occur in real time – USCIS will

not be holding the information for a batched transmission. Upon confirmation of receipt from the UK, the information will be deleted from the USCIS concentrator that has temporarily stored the biometric record pending notice of successful transmission from the UK. USCIS will have no ability to retrieve the information after the confirmation of the successful transfer of the data to the UK. The UK visa applicant population will include third country nationals, Lawful Permanent Residents, and US Citizens. It is anticipated that, routinely, the retention period will be less than 30 minutes and no longer than 12 hours. Although USCIS will not retrieve the information by personal identifier, in the event there is a problem with the transmission, USCIS may need to be able to retrieve the information that is queued up awaiting transmission to determine if the problem is equipment or transmission-related.

Section 1.0
Information collected and maintained

1.1 What information is to be collected?

The information obtained from applicants for the UKvisas project includes biometric, and associated biographic data provided at the time of biometric capture at an ASC. The biometric data includes 10-print fingerprints captured by the electronic live scan device, and photographs. The biographic data includes unique identification, First and Last Name; Date of Birth; Place of Birth; Gender and Aliases. The above data elements will be assembled into an Electronic Fingerprint Transmission Specification (EFTS) file for transmission from the ASC to the UKvisas site in the UK.

1.2 From whom is information collected?

The information is obtained from applicants for UK visas, physically present in the United States at the time of biometric capture. Fingerprints and photos are obtained electronically at one of USCIS' Application Support Centers (ASC). UK visa applicants include third country nationals, Lawful Permanent Residents, and U.S. citizens applying for a UK visa while in the U.S.

1.3 Why is the information being collected?

Section 126 of the UK Nationality, Immigration and Asylum Act of 2002 authorizes the UK to require the submission of biometric information in support of an immigration application. Under Article 3 of The Immigration (Provision of Physical Data) Regulations 2006, the collection of biometric information is required by the UK to enable verification of an applicants' eligibility for a UK visa. In the United States, the UK has a large volume of applications but few locations in which to process them. In order to assist the UK in accomplishing its goals, DHS has agreed to allow its Application Support Centers to perform the services associated with the biometric capture.

1.4 How is the information collected?

An applicant for a UK visa begins the application process by completing the UK visa application on-line at www.visa4uk.gov.uk. The applicant will be directed by the UK to an on-line scheduling system to make an appointment for biometrics capture at a DHS ASC (or, alternatively, at the appropriate UK consulate if the applicant chooses not to submit his or her information at an ASC). The applicant will print the appointment receipt that includes limited biographic data in a bar code. USCIS personnel will scan the

barcode to record the applicant's biographic data into the ASC's livescan biometric capture device. Thereafter, the applicant's biometrics (fingerprints and photograph) will be captured.

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

The Department of Homeland Security has signed a Memorandum of Understanding with the United Kingdom's UKvisas BCP office that defines technical roles, responsibilities, and processes of the two Government agencies in furtherance of the limited gathering and transfer of biometric and biographic information to the UK. Additionally, general authority for the DHS to provide this service to UKvisas BCP on an advanced funds basis is found in section 573 of the Foreign Assistance Act, 22 U.S.C. Section 2349aa, and is also covered by a related letter agreement.

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

Since USCIS is acting solely as an agent for the UK and will be deleting the data as soon as the UK confirms receipt of the information, the privacy risks are extremely limited. Any potential privacy risk associated with the inadvertent disclosure of personally identifiable information is mitigated by the almost instantaneous transfer of the data to the UK utilizing secure encrypted transfer methods, followed by the rapid deletion of the record from USCIS IT systems.

Section 2.0
Uses of the system and the information

2.1 Describe all the uses of information.

USCIS serves only as the front-end data gathering agent for the UK. USCIS will transfer the data to the UK, and the UK government will use the data to determine if the applicant is eligible for a UK visa. After confirmation of receipt by the UK, the information is deleted from USCIS IT systems and cannot be utilized or retrieved by USCIS.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

No.

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

The role of the ASC is strictly a front-end data gathering agent and will not involve performing any data accuracy checks. The ASC personnel will not be required to confirm the identity of the UK visa applicant on behalf of the UK government.

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

USCIS is not using the data for its own purposes. The data submitted by applicants will be deleted as soon as USCIS receives confirmation that the UK has received it.

Section 3.0 Retention

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

USCIS will not retain the data beyond the point at which USCIS has received confirmation that the UK has received the information. USCIS anticipates that the retention period routinely will be less than 30 minutes and will be no longer than 12 hours.

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

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

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

The information is needed for the brief time that it is retained by USCIS in order to ensure a successful transfer. 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 UK. Once

confirmation that the transfer of data was successful, the biometric records will be deleted from the USCIS system.

Section 4.0
Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

USCIS will not be sharing this information with organizations internal to DHS.

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

USCIS will not be sharing this information with organizations internal to DHS.

4.3 How is the information transmitted or disclosed?

USCIS will not be sharing this information with organizations internal to DHS. .

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

USCIS will not be sharing this information with organizations internal to DHS.

Section 5.0
External sharing and disclosure

5.1 With which external organizations is the information shared?

USCIS is acting solely as a data gathering agent of the UK. All such data will be immediately transferred to the UK.

5.2 What information is shared and for what purpose?

All information submitted to USCIS and transferred to the UK will be used by the UK to adjudicate visa application requests.

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

DHS and UK visas BCP have executed an MOU outlining the biometric and limited biographic gathering protocols that USCIS will follow as the front-end agent on behalf of the UK visa issuing program. This PIA covers the first phase of a multi-dimensional information sharing initiative as outlined in the MOU. As additional increments are implemented, DHS will amend applicable privacy related documents.

5.5 How is the shared information secured by the recipient?

USCIS is acting solely as a data gathering point. During the very limited period of USCIS retention data safeguards similar to those applied to all biometric and biographic capture undertaken by USCIS will be employed.

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

The UK government is the owner of this data and they will provide training.

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

The data transfer from USCIS to the UK government will be done through a virtual private network beginning within the DHS firewall and ending within the UKvisas Office firewall.

Section 6.0 Notice

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

This Privacy Impact Assessment (PIA) will be published for the DHS / UKvisas BCP project. Note however that since both the biographic and biometric information that is submitted by persons pursuant to an application for a UK visa is not retrievable from a USCIS IT system by any form of personal identifier, a published system of records notice is not required. Nevertheless, USCIS intends to work with UKvisas to provide notice to individual applicants that USCIS is performing a service for UKvisas, and to inform

applicants about the process by which the information they submit is transmitted to the UK.

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

Applicants who apply for UK visas are required to submit their biometrics and limited biographical information. It will be up to the UK government, not the U.S. government, to determine if an individual has an opportunity to decline to provide the information. It is also not required that an applicant for a UK visa submit his or her information through an ASC; if the applicant chooses, he or she may submit the information directly to the appropriate UK consulate in the United States.

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

USCIS does not use this data. An individual can contact the UK visa office at www.visa4uk.gov.uk if they have any issues relating to the uses of this data.

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

Because USCIS stores this information for very limited period, no privacy risks were identified.

Section 7.0
Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

There is no long-term retention of records by USCIS because USCIS is capturing and transmitting the information on behalf of UKvisas; therefore, USCIS recommends contacting UKvisas directly at www.UKvisas.gov.uk.

7.2 What are the procedures for correcting erroneous information?

See Section 7.1 for further information.

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

See Section 7.1 for further information.

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

See Section 7.1 for further information.

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

There is no long-term storage of the information captured and transmitted by USCIS on behalf of UKvisas. It is recommended that individuals contact UKvisas for additional information.

Section 8.0
Technical Access and Security

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

USCIS personnel at the ASCs who accept the data and who will have limited access to the data until it is deleted. Once the data is transferred to the concentrator housed at a DHS secure technical communication center, a system administrator will have access to the data until the successful transfer of the data to the UK.

8.2 Will contractors to DHS have access to the system?

Yes. Contractors at the ASCs will have access to the livescan biometric capture devices used for data capture. All access to the ASC livescan device systems follows the logical access controls set up for access to USCIS computer systems. Access controls are applied to contractors and to federal employees equally.

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

No. Access to the livescan devices at the ASCs do not use roles. A limited number of individuals have access to the information at the ASCs. Only individuals that have security clearances will have access to the livescan capture devices. The information is controlled by restricting access to individuals who have documented security clearances and who have completed the USCIS computer security awareness training. Additionally, the livescan devices cannot be accessed without a log-in and password.

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

All personnel at the ASCs that have access to the livescan capture devices have security clearances that are documented by the USCIS Office of Security and the ASC Program Office. Additionally, the comprehensive ASC Standard Operating Procedures outlines in detail who has access to these devices.

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

See Section 8.3.

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

The fact that the data is not stored by USCIS should negate the need for any unique safeguards. USCIS insures that access and security controls have been established to mitigate privacy risks associated with authorized and unauthorized users, namely misuse and inappropriate dissemination of data. Audit trails will be kept in order to track and identify unauthorized uses of system information. Further, the ASCs comply with the DHS security guidelines, which provide hardening criteria for securing networks, computers and computer services against attack and unauthorized information dissemination.

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

Training on the livescan capture devices at the ASCs will be provided to ASC personnel who have access. This training will address appropriate privacy concerns. In addition, ASC employees and contractors who have been granted appropriate access by a superior, will be assigned a login and password to access the system. These users will have previously undergone federally approved clearance investigations and signed appropriate documentation in order to obtain the appropriate access levels. In addition, every Federal employee and contractor is required to take annual computer security awareness training.

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

The ASCs are currently engaged in the Certification and Accreditation process with the appropriate USCIS OCIO security staff. The ASCs currently have a temporary Authority to Operate.

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

Since the information is stored at USCIS for such a short period of time, the privacy risks are minimal. Even though these risks are minimal, USCIS insures that access and security controls have been established to mitigate privacy risks associated with authorized and unauthorized users, namely misuse and inappropriate dissemination of data. Audit trails will be kept in order to track and identify unauthorized uses of system information. Further, the ASCs comply with the DHS security guidelines, which provide hardening criteria for securing networks, computers and computer services against attack and unauthorized information dissemination.

Section 9.0 Technology

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

This process is utilizing the existing ASC infrastructure. The only deviation from the existing protocol is the routing of the UKvisas records through DHS' secure network directly to the UK.

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

The biometrics and biographical information that are being gathered on behalf of the UK are being stored for an extremely limited period of time in a USCIS system.

9.3 What design choices were made to enhance privacy?

The biometrics and biographical information that are being gathered on behalf of the UK are being stored for an extremely limited period of time in an USCIS system.

Responsible Officials

Elizabeth Gaffin, USCIS, Privacy Office

Department of Homeland Security

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security