



Privacy Impact Assessment
for the

United States Visitor and Immigrant Status Indicator
Technology Program/Department of Homeland Security
and the United Kingdom Border Agency's International
Group Visa Services Project

July 2, 2008

Contact Point

**Paul Hasson, Acting Privacy Officer
US-VISIT Privacy
(202) 298-5200**

Reviewing Official

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



Abstract

For this project, the U.S. Department of Homeland Security (DHS) will provide the United Kingdom Border Agency's (UKBA) International Group Visa Services (formerly known as UKvisas) with additional information to determine whether visa applicants for entry into the United Kingdom are eligible to obtain a visa or other travel documents according to applicable United Kingdom laws. Accordingly, the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program will receive biometric and biographic information from UKBA International Group Visa Services about applicants for visas to the United Kingdom and will query those applicants' biometric information against the Automated Biometric Identification System's (IDENT)¹ 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.) US-VISIT will provide UKBA with results from the query, along with, in some cases, details of the analysis supporting the returned results. US-VISIT is publishing this privacy impact assessment (PIA) because US-VISIT will receive and share personally identifiable information (PII) with the UKBA.

Overview

The DHS and UKBA International Group Visa Services Project is multiphased and requires the support of U.S. Citizenship and Immigration Services² (USCIS), the US-VISIT Program, on behalf of DHS, and UKBA International Group Visa Services posts (i.e., embassies and consulates) located within the United States on behalf of the UKBA. In this phase of the project, DHS will provide certain information to UKBA International Group Visa Services to assist UKBA in its determination as to whether visa applicants for entry into the United Kingdom are eligible to obtain a visa or other travel documents according to applicable United Kingdom laws.

To obtain a visa to enter the United Kingdom, all applicants must submit biographic and biometric information. The United Kingdom uses the information submitted by the applicant to determine whether the applicant is eligible for the visa sought. Specifically, visa applicants must submit their visa application forms online to the UKBA.³ Part of the visa application involves submitting biometric information in addition to the biographic and travel information required for the online application. Applicants must present themselves with a photo identification to a USCIS Application Support Center (ASC) or an UKBA International Group Visa Services post

¹ DHS republished the system of records notice (SORN) for IDENT in the Federal Register on June 5, 2007 (Vol. 72, Number 107, Page 31080-31082) which replaces the previously published SORN that appeared in the Federal Register on July 27, 2006 (71 FR 42651). The original and republished Privacy Impact Assessment (PIA) for IDENT can be found at the DHS website (www.dhs.gov/privacy).

² USCIS has published a Privacy Impact Assessment addressing its role in the DHS/UKvisas Project (November 14, 2007) http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_ukvisa.pdf.

³ The United Kingdom Border Agency International Group Visa Services online application system can be found at www.ukvisas.gov.uk/.



to provide their biometrics (e.g., fingerprints and digital facial photographs). The ASC will provide the biometric data to the UKBA for processing. The UKBA will then compare the biometric data to its own biometric repository and will send the biometric data to US-VISIT for comparison against a subset of IDENT fingerprints.

US-VISIT will receive only biometric and limited biographic visa application information from UKBA. This information will be queried against the IDENT 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). If a match to any entry within the IDENT list of subjects of interest occurs, US-VISIT will verify the match at their biometric support centers (BSC) by a certified fingerprint examiner. Upon verification, US-VISIT will forward the notification of the match for the record to UKBA International Group Visa Services and to US-VISIT’s identity services group. As a result of a match, further sharing of information may occur between UKBA International Group Visa Services and DHS to resolve any discrepancies or investigate a match for law enforcement or intelligence purposes. In such cases, the information UKBA International Group Visa Services provides to US-VISIT will be retained by the identity services group under the Technical Reconciliation Analysis Classification System (TRACS) system of records notice last published June 16, 2008 73 FR 34028, and handled in accordance with that SORN and any other necessary law enforcement or immigration procedures.

Typical Transaction

The UKBA International Group Visa Services process begins when an individual who is physically located within U.S. borders submits a visa application to enter the United Kingdom. Applicants will complete the online portion of the application⁴ and, upon confirmation from the UKBA, will receive authorization to present themselves to a USCIS ASC or an UKBA International Group Visa Services post to provide biometric and limited biographic information. All data is returned to the UKBA, which in turn forwards the biometric data to IDENT, as described above, for queries against a list of subjects of interest.

In this typical transaction, if a match occurs, the match is identified using IDENT⁵ and analyzed and verified at the BSC and retained using TRACS⁶. Any additional information provided by UKBA will also be stored in TRACS. If no match occurs, the UKBA will be notified and no data or information will be retained by US-VISIT.

If this project is expanded in the future, any changes that affect the handling of PII will be documented in a new or revised PIA in accordance with the E-Government Act of 2002.

⁴ As stated above, found at www.ukvisas.gov.uk.

⁵ No UKBA International Group Visa Services data will be stored in IDENT.

⁶ TRACS is an information management tool used for the storage and analysis of DHS records by US-VISIT.



Section 1.0 Characterization of the Information

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

1.1 What information is collected, used, disseminated, or maintained in the system?

Initial Collection and Transmission to UKBA and US-VISIT for Query within IDENT

US-VISIT does not collect any biometric or biographic information from the UKBA International Group Visa Services applicants directly. Applicants submit their biographic information via the UKBA online visa application. Additionally, the applicant submits their biometric data (i.e., 10 fingerprints and digital facial photograph) at a USCIS ASC or an UKBA International Group Visa Services post. The following categories of information are required to complete the UKBA visa application:

- Ten fingerprints
- Digital facial photograph
- Full name (i.e., first, last, middle, nickname, and alias)
- Date of birth
- Place of birth
- Citizenship
- Document identifier (e.g., document type, document number & country of issuance)
- Gender

The UKBA International Group Visa Service group then forwards the applicant's information with the addition of the UK unique ID number to US-VISIT. Only the biometric data (i.e., 10 fingerprints) will be queried against the IDENT list of subjects of interest, name based checks will not be conducted.

If a match does *not* occur, US-VISIT will transmit two data elements back to the UK:

- a) Status code: "None"
- b) UK Unique Identifier.

US-VISIT will delete all information pertaining to the applicant.

If a match *does* occur, US-VISIT will transmit three data elements back to the UK:

- a) status code: "Watchlist"
- b) UK Unique Identifier
- c) Encounter ID.

The applicant's information will be enrolled into TRACS for case management.

Further Information Sharing between US-VISIT and UKBA in the event of a Match



If the applicant's information matched with IDENT data then US-VISIT will enroll the applicant's information into the TRACS case management system. TRACS information may be shared with the UK, other foreign, US local, State, tribal, and Federal government and law enforcement agencies. Upon receipt of a match, a UKBA analyst may contact a US-VISIT analyst to obtain this additional information about the applicant and may provide additional information to US-VISIT about the applicant.

TRACS⁷ will contain at a minimum the following data elements:

- Full Name(s)
- Encounter ID
- Data of birth
- Country of birth
- Event Date
- Event Time
- Terminal ID
- Site code
- Fingerprint Identification Number (FIN)
- FBI number
- Critical refusal
- Wanted records
- Interpol records
- Comments

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

Applicants for a visa to enter the United Kingdom are required to provide a minimal set of biographic (name, date of birth, sex, nationality, and passport number) and biometric (10 fingerprints and a digital facial photograph) data. The majority of those applying in the United States for a visa to enter the United Kingdom will be third-country nationals. However, U.S. citizens (USCs)⁸ who intend to stay in the United Kingdom for longer than three months, or to enter the United Kingdom to engage in work, may also require a visa, according to U.K. immigration laws.

The 10 fingerprints provided by the visa applicant are compared to the IDENT list of subjects of interest, a subset of the IDENT database. If the applicant's fingerprints match any of these subset of prints in IDENT, US-VISIT may request and receive from UKBA International Group Visa Services additional biographic information from other U.K. immigration systems not already provided by the applicant.

⁷ All data elements collected, maintained, and disseminated in TRACS can be viewed in the TRACS PIA at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_tracs.pdf

⁸ US-VISIT does not intentionally collect information on U.S. citizens for IDENT outside of the scope of the United Kingdom Border Agency International Group Visa Services project.



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

US-VISIT will use the biographic and biometric information received from UKBA International Group Visa Services, and provided by the visa applicant, to determine whether the applicant's biometrics are currently included in the IDENT list of subjects of interest. In the event of a biometric match, US-VISIT will use additional biographic information provided by the United Kingdom to support any necessary law enforcement or immigration enforcement investigations. UKBA International Group Visa Services will use the biometric and biographic information provided by the visa applicant, and the information regarding the query of the visa applicant, to compare with the IDENT list of subjects of interest as part of its visa adjudication process.

If there is no biometric match from the UKBA International Group Visa Services application against the IDENT list of subjects of interest, US-VISIT will not retain any biometric or biographic information from UKBA International Group Visa Services applicants. If there is a biometric match against the IDENT list of subjects of interest, US-VISIT may request and receive from UKBA International Group Visa Services additional biographic information not already provided by the applicant from other U.K. immigration systems. All data pertaining to a match of a UKBA International Group Visa Services applicant's information against the IDENT list of subjects of interest will be retained in the TRACS, an information management tool used by US-VISIT to enhance the integrity of the U.S. immigration system by detecting, deterring, and pursuing immigration fraud, and to identify persons who pose a threat to national security and/or public safety. IDENT data is not updated, modified, or altered in anyway. US-VISIT will use IDENT to only read/search its gallery not write data to it.

1.4 How is the information collected?

Initial Collection and Transmission to UKBA and Query Within IDENT

The information will be provided by the visa applicant at the USCIS ASC or at the UKBA International Group Visa Services post. The visa applicant will submit a minimal set of biographic and biometric data. The set of biographic data will be collected on the visa application; the collection of fingerprints will be captured on existing electronic fingerprint capturing hardware at ASCs and UKBA International Group Visa Services posts; and the photograph will be captured via a digital camera at ASCs and UKBA International Group Visa Services posts.

After an applicant's information is collected at an ASC or a UKBA International Group Visa Services post, it will be transmitted to UKBA International Group Visa Services via a secure dedicated telecommunications circuit. Subsequently, fingerprints and minimal biographics will be transmitted to US-VISIT from UKBA International Group Visa Services via a secure dedicated telecommunications circuit.



Further Information Sharing between US-VISIT and UKBA in Case of Match

In the event of a match, UKBA International Group Visa Services will receive additional data from DHS on the applicant, and US-VISIT may receive additional information regarding the applicant from UKBA International Group Visa Services. All data transfers between the involved entities will only occur over secured dedicated telecommunications circuits.

If no match occurs to the US-VISIT IDENT database, the biometric and minimal biographic data is not retained by US-VISIT.

1.5 How will the information be checked for accuracy?

The biographic and biometric information necessary for a UKBA International Group Visa Services application will be collected directly from the individual at an ASC or a UKBA International Group Visa Services post and securely transferred to UKBA International Group Visa Services to promote the accuracy of the information. Biometric and limited biographic data collected in the United States will be transmitted by a separate process from UKBA International Group Visa Services to US-VISIT for query against IDENT.

In the event of a match against the IDENT list of subjects of interest, IDENT performs certain quality checks (e.g., a certified fingerprint examiner at the BSC verifies the match, and also determines the quality of a fingerprint captured and its suitability for matching in the future) and seeks to ensure that the data meets a minimum level of quality and completeness. Any additional information shared between DHS and UKBA International Group Visa Services following a match with the list of subjects of interest will be transmitted through secure communications to mitigate the risk of unauthorized access or modification of the information.

US-VISIT also promotes the accuracy of the information by providing UKBA International Group Visa Services applicants the opportunity to amend erroneous information in their records, as discussed in Section 7.1 of this PIA.

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

DHS and the UKBA International Group Visa Services' Biometrics Capture Programme office, a joint directorate of the Foreign and Commonwealth Office and the Border and Immigration Agency, have entered into agreements that define the roles, responsibilities, and processes of these agencies in the collection and transfer of biometric and biographic information to the United Kingdom and the return of a subset of that information to the United States for comparison against the IDENT subjects of interest list and consequent research into and sharing of information concerning matches. General authorities for DHS to pursue the DHS/UKBA International Group Visa Services project include the Immigration and Nationality Act (8 U.S.C.



1101 et. seq.), the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Public Law 107-56 (as amended), and the Foreign Assistance Act of 1961, Public Law 87-195 (as amended).

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

Since the DHS/UKBA International Group Visa Services project involves the collection of PII from a new category of individuals (i.e., U.K. visa applicants) for a new instance of data sharing and processing between the United States and the United Kingdom, US-VISIT reviewed the UKBA International Group Visa Services project to ensure that the data could be collected and processed in relevant systems. Accordingly, the biometrics and biographics being collected by the UKBA International Group Visa Services project will be covered under the System of Records Notices (SORNs) for IDENT⁹ and TRACS¹⁰. While the population of UKBA International Group Visa Services applicants will principally include aliens who are not legal permanent residents (LPRs), it will also include both LPR and USCs, and no distinction will be made on the basis of U.S. citizen or LPR status for the purposes of vetting against the IDENT list of subjects of interest. Therefore, US-VISIT may receive, use, and retain such information in IDENT and TRACS as outlined by standard operating procedures and governing agreements. For example, if a biometric match against the IDENT list of subjects of interest is verified, then the applicant's information is retained by US-VISIT in TRACS.

In identifying which types of information were required for the initial matching against IDENT, US-VISIT and UKBA identified the minimum amount of information required to conduct an accurate match. US-VISIT and UKBA will only then share additional information if there is a match. Where there is no match, US-VISIT does not maintain the information received from UKBA beyond the initial processing. Both of these processes minimize the privacy risk of more information being collected than is necessary to perform the program.

US-VISIT also reviewed the UKBA International Group Visa Services project to ensure that the search and potential subsequent sharing of IDENT list of subjects of interest data was conducted in accordance with the privacy requirements that govern the initial collection of the IDENT list of subjects of interest data. Accordingly, US-VISIT has agreements in place with IDENT stakeholders/data owners from the U.S. Government agencies that maintain the data on the IDENT list of subjects of interest to search that data and to coordinate the subsequent sharing of additional information. However, in the event of a match, some data owners require US-VISIT to share with them the hit information and the information the fact that we are going to share with the UKBA International Group Visa Services project prior to transmitting the information. This step will allow the data owner to verify the information is complete and

⁹ [DHS Automated Biometric Identification System \(IDENT\)](#) DHS/USVISIT-0012, June 5, 2007, 72 FR 31080

¹⁰ DHS Technical Reconciliation Analysis Classification System (TRACS) DHS/USVISIT-003, June 16, 2008, 73 FR 34028



accurate.

Specific requirements outlined by the U.S. Government will comply with all appropriate laws, regulations, policies, and agreements. For example, the PII retained in TRACS as the result of an IDENT list of subjects of interest match can be shared with appropriate U.S. Government agencies for law enforcement or immigration enforcement investigation.

Furthermore, the data used in the DHS/UKBA International Group Visa Services project is collected, shared, and transferred via secure means to mitigate the risk of unauthorized access or modification of the data. Once the data is received by US-VISIT, it is protected through the robust privacy and security programs discussed further in Section 8 for the relevant US-VISIT systems.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

Upon receipt of the UKBA International Group Visa Services applicant's biometric information, US-VISIT will query the applicant's biometric data against the IDENT list of subjects of interest. If there is no match when the applicant's biometric information (i.e., 10 fingerprints) is queried to the IDENT list of subjects of interest, then UKBA International Group Visa Services is notified of the search results. All records that do not match to the IDENT list of subjects of interest are purged immediately after transmission of the search results to UKBA International Group Visa Services. UKBA uses the results of this query to identify whether the applicant may be ineligible for a visa.

If there is a match when the applicant's biometric data is queried against the IDENT list of subjects of interest information, US-VISIT will verify the match at the BSC. Upon verification, US-VISIT will notify the UKBA International Group Visa Services of that match. UKBA International Group Visa Services will receive from US-VISIT any available information related to the applicant in accordance with established procedures.

If a match against the IDENT list of subjects of interest occurs, US-VISIT will use TRACS to collect and monitor the data from its source systems when necessary to support the analyses, investigations, and management of cases to control illegal immigration, fraud, inquiries, encounters, and investigative referrals.

The match information from UKBA and IDENT will be compiled in TRACS with other relevant information such as that from the Arrival and Departure Information System. TRACS may also contain information from other systems checked while researching a particular case. If



research is based on an external request, information may be provided from the requesting entity. These systems include, but are not limited to:

1. DHS Customs and Border Protection (CBP) Treasury Enforcement Communications System (TECS)
2. Department of State Consolidated Consular Database (CCD)
3. DHS Immigration and Customs Enforcement (ICE) Student and Exchange Visitor Information System (SEVIS)
4. USCIS Central Index System (CIS)
5. USCIS Computer-Linked Application Information Management System (CLAIMS 3 and 4)
6. USCIS Refugees, Asylum, and Parole System (RAPS)
7. ICE Deportable Alien Control System (DACs)
8. ICE Enforcement Case Tracking System (ENFORCE)¹¹
9. Public information from Web searches for addresses and telephone numbers

For more information about TRACS refer to the TRACS PIA located on the DHS Web site: www.dhs.gov/privacy.

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

US-VISIT will use existing analytical tools established for IDENT and TRACS. Biometric data received from UKBA International Group Visa Services is queried against the IDENT database. If a match occurs, additional biographic data received from UKBA International Group Visa Services is moved into TRACS. Through TRACS, US-VISIT can then provide technical assistance and analytical services to UKBA International Group Visa Services by monitoring the data from its source systems when necessary to support the analyses, investigations, and management of cases to control illegal immigration, fraud, inquiries, encounters, and investigative referrals. There is no change to the types of tools used to analyze the data in IDENT or TRACS.

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

The biometric and biographic data that is checked against IDENT is provided directly to UKBA International Group Visa Services by the visa applicant and does not come from any

¹¹ 66 FR 53029, Treasury Enforcement Communication System, System of Records Notice, October 18, 2001; 70 FR 14477, Student and Exchange Visitor Information System, System of Records Notice, March 22, 2005; 72 FR 1755, Central Index System, System of Records Notice, January 16, 2007; 67 FR 64132, Computer Linked Application Information Management System, System of Records Notice, October 17, 2002; and 67 FR 64136, Deportable Alien Control System, System of Records Notice, October 17, 2002.



commercial or publicly available data source.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

To protect against the misuse of data, US-VISIT purges any information that is not relevant to DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions. Specifically, US-VISIT does not retain any PII from UKBA International Group Visa Services applicants that does not match an entry on the IDENT list of subjects of interest or require additional law enforcement or immigration enforcement investigation.

US-VISIT employs strong privacy and security protections to reduce the likelihood of unauthorized use or modification of its data, including data received from UKBA International Group Visa Services. In addition, physical, technical, and administrative access controls are applied, along with user education and the necessary training to sustain the confidentiality of the collected PII. PII collected in those systems is not to be discussed with, nor disclosed to, any person within or outside US-VISIT other than as authorized by law and as required for the performance of official duties. A program-dedicated Privacy Officer ensures that the data is not used or accessed improperly and the DHS Chief Privacy Officer continues to exercise oversight of US-VISIT to ensure that the information collected and stored in US-VISIT systems is properly protected under current privacy laws and guidance.

The US-VISIT security policy, discussed further in Section 8.0, requires that the confidentiality and integrity of an individual's personal information be maintained. Accordingly, the systems supporting the DHS/UKBA International Group Visa Services project are validated through a Certification and Accreditation (C&A) process on a regular basis. IDENT was granted an authority to operate (ATO) in May 2007; that ATO is set to expire in May 2010. TRACS is currently under development and is in the C&A process as of the publication date of this PIA. As discussed above, users of these systems have limited access that is based on their roles and they are trained in the handling of personal information.

Moreover, US-VISIT acts as the data steward for those U.S. Government agencies that maintain data on the IDENT list of subjects of interest, ensuring that the DHS/UKBA International Group Visa Services project complies with the privacy requirements governing the initial collection of list of subjects of interest data. Accordingly, US-VISIT will seek permission from the U.S. Government agencies that maintain the data on the IDENT list of subjects of interest to search that data and to coordinate the subsequent sharing of additional information. The specific requirements outlined by those U.S. Government agencies serve as the basis for the handling procedures for such data as well as all appropriate laws, regulations, policies, and data-sharing arrangements.



Section 3.0 Retention

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

3.1 How long is information retained?

If the visa applicant's information does not match with the IDENT list of subjects of interest records, then the applicant's information is not retained by US-VISIT.

If the visa applicant's information matches the IDENT list of subjects of interest, US-VISIT will retain the biographic information received from UKBA International Group Visa Services in TRACS. IDENT data is not updated, modified, or altered in anyway. US-VISIT will use IDENT to only read/search its gallery, not write data to it.

The applicants' information will be retained in TRACS only until any U.S. administrative or law enforcement action against the visa applicant has concluded (including all appeal periods), or a request has been made by UKBA International Group Visa Services that the information be destroyed in order for UKBA International Group Visa Services to meet its statutory requirements. In any event, US-VISIT intends to destroy the information within 10 years of its receipt from UKBA International Group Visa Services unless the information is being maintained by a court of the United States or is otherwise required to be maintained by U.S. law. Pursuant to section 5, viii., of the memorandum of understanding between the DHS and UKBA International Group Visa Services, US-VISIT will not be required to destroy information in TRACS or provide for the destruction of documents maintained by a court of the United States, nor shall it require the destruction of a document which is required to be maintained by U.S. law. UKBA International Group Visa Services will retain the information provided by DHS until such time that UKBA International Group Visa Services has no mission-related need or for up to 75 years of its receipt from DHS, whichever is sooner.

3.2 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration?

The retention schedule has been approved for IDENT and is subject to revision if necessary. The retention schedule for TRACS is currently in development with the National Archives and Records Administration.

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

When PII is retained, there is a risk that the data will be kept longer than necessary for



the use governing its initial collection or longer than its authorized retention period, and that the data may become vulnerable to unauthorized access, use, and disclosure. Accordingly, US-VISIT has sought to minimize the retention period for the data exchanged with UKBA International Group Visa Services as necessary to support the purposes of law enforcement, immigration and border management, and national security for which the DHS/UKBA International Group Visa Services project was created.

The retention period described in section 3.1 balances the need for the information for records control purposes, including in any U.S. administrative or law enforcement action against the visa applicant through conclusion, with the U.K. interest underlying its statutory requirements to destroy the information.

UKBA International Group Visa Services will retain the information it receives from US-VISIT until such time that UKBA International Group Visa Services has no mission-related need for retention, or within 75 years of its receipt from DHS. The 75-year retention period is necessary to support the holding of biometrics of subjects of interest in immigration and border management or law enforcement activities.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared, and for what purpose?

If an applicant's biometric information matches against the IDENT list of subjects of interest during the routine query, then results from this match will be enrolled in TRACS and shared with DHS users such as US Citizenship and Immigration Services (CIS), Immigration and Customs Enforcement (ICE), Intelligence and Analysis (I&A), and Customs and Border Protection (CBP) as appropriate and permissible. Components within DHS and other US Federal Government agencies with which IDENT data is shared are usually responsible for preparing a PIA that describes the specifics of that sharing and are published accordingly.

US-VISIT shares data contained in IDENT and TRACS, with the consent of the data owner, for purposes of national security, law enforcement, immigration, intelligence, and other DHS mission-related functions, and to provide associated testing, training, management reporting, planning, and analysis, or other administrative uses that require the use of biometrics to identify or verify the identity of individuals.

4.2 How is the information transmitted or disclosed?

In most cases the data is transmitted between IDENT and other systems on the DHS core



network -- an unclassified, secured wide-area network. All data transmitted or disclosed among U.S. Government agencies as a result of the DHS/UKBA International Group Visa Services project will occur via secured communications.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

In many cases, DHS internal data sharing is required to comply with statutory requirements for national security and law enforcement. In all cases, however, this data must be kept secure, accurate, and appropriately controlled. Data owners ensure that any privacy risks are mitigated through data-sharing agreements or arrangements that require auditing, access controls, resharing limits, and other physical, technical, and administrative controls.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, State, and local governments, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

The UKBA International Group Visa Services office will receive all data elements that were collected in the UKBA International Group Visa Services application. UKBA International Group Visa Services will receive all results generated by IDENT during the visa adjudication process. Further, if a match has been generated by querying the applicant's fingerprint data to the IDENT list of subjects of interest, then TRACS will maintain information pertaining to the applicant. Subsequently, US-VISIT will transmit additional information associated with the applicant's record to the UKBA International Group Visa Service, in accordance with established agreements between US-VISIT or DHS and the owner of the additional data.

US-VISIT may share information with appropriate Federal, State, local, tribal, foreign, or international government agencies charged with national security, law enforcement, immigration, intelligence, or other DHS mission-related functions.



5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The sharing of a visa applicant's biographic and biometric information is consistent with the original purpose for which it was collected. The SORNs for IDENT and TRACS have provisions for sharing data with foreign governments for national security, law enforcement, intelligence, and other DHS-mission related functions.

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

There is a secure transmission medium between the ASCs to UKBA International Group Visa Services and from UKBA International Group Visa Services to US-VISIT IDENT, which receives, processes, and generates results for an IDENT subject of interest list query. Results for the IDENT list of subjects of interest query are transmitted to UKBA International Group Visa Services via a secure, encrypted e-mail transmission. The e-mail encryption complies with the encryption standards of the Department of Commerce's National Institute of Standards and Technology, which are used to secure personal and other sensitive information.¹²

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

Data shared with UKBA International Group Visa Services must be kept secure, accurate, and appropriately controlled through auditing, access controls, resharing limits, and other physical, technical, and administrative controls. Security is maintained by using secure transmission media that prevent unauthorized access and that sustain information confidentiality and integrity. Data owners are responsible for ensuring that any privacy risks are mitigated.

In accordance with its SORNs, US-VISIT may share data contained in IDENT and TRACS, with the consent of the data owner, for purposes of national security, law enforcement, immigration, intelligence, and other DHS mission-related functions.

¹² *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards 140-2 National Institute of Standards and Technology (May 25, 2001).



Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Notice regarding the collection of information is provided to an individual prior to the collection through USCIS ASCs, the USCIS PIA title UKVisas Project published November 14, 2007, and the UKBA International Group Visa Services Web site. In addition, the UKBA International Group Visa Services visa application form advises the applicant that data provided in connection with the application may be shared with foreign governments.

Additionally, the collections are covered by the system of records notice for IDENT, DHS/USVISIT-0012, June 5, 2007, 72 FR 31080 for the initial processing and for TRACS DHS/USVISIT-003, June 16, 2008, 73 FR 34028 for records that have a possible match to an IDENT list of subjects of interest information.

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

The UKBA International Group Visa Services application process is a requirement for all individuals who need a visa to enter the United Kingdom. To enable appropriate consideration of an application, applicants must provide the necessary information.

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

Individuals do not have the right to consent to a particular use of their information once they submit applications for visas to enter the United Kingdom. Upon submission of their completed applications, the information is subject to identity verification and query against the IDENT list of subjects of interest.



6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

If individuals require a visa to enter the United Kingdom, there is no opportunity or right to decline to provide their information nor a right or opportunity to limit its use. If the applicant is denied a visa to enter the United Kingdom, UKBA International Group Visa Services will provide a letter of visa denial and visa appeal to the applicant. The UKBA International Group Visa Services appeals process varies based on the circumstances upon which the applicant was denied a visa. The letter will detail the process the applicant must follow in order to appeal the visa decision.

Given the number of government actors involved in the DHS/UKBA International Group Visa Services project, there is a risk that individuals may not understand what data is being collected, by whom, and for what purpose. Accordingly, UKBA International Group Visa Services, USCIS, and US-VISIT intend to work together with the visa applicant if necessary, to provide notice of process and applicable procedures explaining the U.K. visa application process. Public notice is also provided through the USCIS PIA for the UKBA International Group Visa Services project, which was approved on November 14, 2007, on the Ukvisas web site.

Section 7.0 Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

US-VISIT information may, in some cases, be exempt from individual access because access to the data in IDENT and TRACS could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, or to the existence of the investigation, and could reveal investigative interest on the part of DHS or another agency. In those cases, access to records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. However, in many other cases, individuals may request and receive access by submitting a request to the US-VISIT Privacy Officer, US-VISIT Program, U.S. Department of Homeland Security, Washington, D.C. 20528.

If the applicant is denied a visa to enter the United Kingdom, UKBA International Group Visa Services will provide a letter of visa denial and visa appeal to the applicant. The UKBA International Group Visa Services appeals process varies based on the circumstances upon which the applicant was denied a visa. The letter will detail the process the applicant must follow in



order to appeal the visa decision.

7.2 What are the procedures for correcting inaccurate or erroneous information?

To correct inaccurate or erroneous information maintained in a DHS system, individuals may submit a redress request through the DHS Traveler Redress Inquiry Program (TRIP) Web site at www.dhs.gov/trip. Once an individual submits a redress request, the individual will receive notification of receipt. DHS TRIP will review the redress request and will coordinate with US-VISIT, which will then review the individual's records and correct the information, if appropriate. The individual will then receive notification from DHS TRIP regarding the resolution to his or her request.

It is important to note that DHS TRIP and US-VISIT cannot influence the UKBA International Group Visa Services visa adjudication process. UKBA International Group Visa Services is solely responsible for granting or denying UKBA International Group Visa Services applications. UKBA International Group Visa Services will determine whether any change to an applicant's information by US-VISIT, as a result of a successful redress request, will impact the adjudication process of UKBA International Group Visa Services. The appeals process for handling inaccurate or erroneous information, on behalf of the UKBA International Group Visa Services program, is solely the responsibility of the UK and can be found on their website.¹³

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

The UKBA International Group Visa Services application provides notice of the procedures to access and redress information within TRIP. The notice will instruct individuals to seek redress from DHS/TRIP if they believe that their personal information held by DHS is incorrect. If a visa applicant is denied a visa to the United Kingdom, UKBA International Group Visa Services will provide a rejection letter and an appeal process notice to the applicant. The rejection letter will state under which circumstances the visa application was denied and, if appropriate, will provide an opportunity to appeal the decision.

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

If redress cannot be provided, or if the individual is dissatisfied with the response received from US-VISIT, the individual can appeal his or her case to the DHS Chief Privacy Officer, who will review the appeal and provide final adjudication concerning the matter. The

¹³The UKBA International Group Visa Services appeals process can be located at: <http://www.ukvisas.gov.uk/en/howtoapply/infs/inf19appeals>



DHS Chief Privacy Officer can be contacted at Chief Privacy Officer, Attn: US-VISIT Appeal, U.S. Department of Homeland Security, Washington, D.C. 20528, USA; or by fax: 00-1-202-772-5036.

UKBA International Group Visa Services has its own access and appeal process, which is detailed in the visa decision and visa appeal letters provided to the applicant. More information can be found by the applicant on the UKBA International Group Visa Services Web site at www.ukvisas.gov.uk/.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Given the number of government entities involved in the DHS/UKBA International Group Visa Services project, there is a risk that UKBA International Group Visa Services applicants may not know that a redress process exists for DHS information or how redress differs from an appeal of the visa decision. Accordingly, US-VISIT and UKBA International Group Visa Services intend to work together to notify individuals of DHS TRIP throughout the UKBA International Group Visa Services application process and through this Privacy Impact Assessment.

DHS TRIP provides a redress process that furthers the privacy interest of the individual by providing an easy-to-use Web site that provides a central point of contact for the submission and processing of redress requests. DHS TRIP collects PII directly from the individual, and therefore the risk of collecting inaccurate information should be minimized. PII submitted to DHS TRIP will be protected and will only be shared in accordance with the provisions of the Privacy Act of 1974 (5 U.S.C. § 552a) and as provided in the DHS TRIP Privacy Impact Assessment, published January 18, 2007. In addition, individuals may request access to or correction of their PII pursuant to the Freedom of Information Act or the Privacy Act, as appropriate.

It is important to note that DHS TRIP and US-VISIT cannot influence the UKBA International Group Visa Services visa adjudication process. UKBA International Group Visa Services is solely responsible for granting or denying UKBA International Group Visa Services applications. UKBA International Group Visa Services will determine whether any change to an applicant's information by US-VISIT, as a result of a successful redress request, will impact the adjudication process of UKBA International Group Visa Services. The appeals process for handling inaccurate or erroneous information, on behalf of the UKBA International Group Visa Services program, is solely the responsibility of the UK and can be found on their website.¹⁴

¹⁴The UKBA International Group Visa Services appeals process can be located at: <http://www.ukvisas.gov.uk/en/howtoapply/infs/inf19appeals>



Section 8.0 Technical Access and Security

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

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

DHS has documented standard operating procedures to determine which users may access systems that support US-VISIT. To access these systems, users must hold the appropriate security clearance, perform a clearly defined role requiring access to the information in the system, and receive mandatory security and privacy training. The clearance, job responsibilities, and mandatory security and privacy training activities for all individuals permitted access to US-VISIT systems are documented and maintained to reflect changes in user status and responsibilities. Access is then granted on the principles of least privilege, separation of duties, and need to know. A user's "need to know" depends on the context of when, how, and why the user requires access to information. Accordingly, "need to know" is asserted by the user after the other procedures to obtain access have been established, and that assertion is validated and confirmed by the user's manager, the system manager, and security personnel. Event logs record system access and the Information Systems Security Manager confirms compliance to policy and manages the activation or deactivation of accounts and privileges as required or when expired.

Access control procedures operate in conjunction with a robust security program that implements physical, administrative, and technical controls to protect the confidentiality, integrity, and availability of the system.

8.2 Will Department contractors have access to the system?

In accordance with the access policies and procedures established by DHS, contractors will have access to the systems that support the US-VISIT DHS/UKBA International Group Visa Services project, including IDENT and TRACS, to perform their official duties, such as system administration, monitoring, and security functions. Contractor access will be granted in accordance with the principles of least privilege, separation of duties, and need to know. The access policies and logs will be reviewed by security management to ensure the effective implementation of privacy and security safeguards.



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

All users of Government systems supporting US-VISIT receive privacy training prior to obtaining access to those systems. DHS personnel, including Government personnel and contractors, are required to take mandatory privacy training offered by their DHS component. US-VISIT personnel receive instruction on privacy regulations and legislation, the responsibilities of the US-VISIT Privacy Team, and the privacy rules of behavior governing the performance of professional duties. Users external to DHS, who are parties to data-sharing arrangements, are also required to receive privacy training in accordance with other agreements authorizing the sharing of data.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The data is secured in accordance with DHS and Federal security requirements, including Federal Information Systems Management Act requirements. IDENT was granted an authority to operate in May 2007; unless reaccruited, this authority to operate will expire in May 2010. TRACS is currently under development and is undergoing the C&A process.

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

The PII received by US-VISIT for the DHS/UKBA International Group Visa Services project is subject to appropriate technical safeguards and audit capabilities of the systems in which the PII is stored. US-VISIT secures information and the systems on which that information resides by complying with the requirements of DHS information technology security policy. As part of implementing policy and meeting information assurance and privacy requirements, US-VISIT maintains an audit function that tracks all user activities related to data, including access and modification. These procedures and access logs are subject to management oversight that confirms compliance with privacy and security requirements. US-VISIT also seeks to prevent unauthorized access to data stored in its supporting systems through technical controls, including firewalls, intrusion detection, encryption, access control lists, system hardening techniques, and Interagency Security Agreements (ISAs) that document controls for external connections, among other security methods. Periodically, US-VISIT and the systems on which its information resides are evaluated to ensure compliance with mandated privacy and security requirements.

Because US-VISIT systems contain data from a variety of sources, collected for a variety of uses, it is necessary to implement appropriate controls so that only those individuals making appropriate use of the data are able to access that data. US-VISIT systems have a robust set of



access controls, including role-based access controls and interfaces that limit access to appropriate and discrete data collections. Misuse of data in US-VISIT systems is prevented or mitigated by requiring that users conform to appropriate security and privacy policies, follow established rules of behavior, and be adequately trained regarding the security of their systems. Also, a periodic assessment of physical, technical, and administrative controls is performed to enhance accountability and data integrity. External connections must be documented and approved with both parties' signatures in an ISA, which outlines the controls in place to protect the confidentiality, integrity, and availability of information being shared or processed.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

US-VISIT mitigates the risk of unauthorized access to DHS systems through the use of encrypted communication links between UKBA International Group Visa Services and IDENT, boundary protection within the DHS core network, and access control and other management, operational and technical security processes within IDENT, TRACS and other US-VISIT support systems. Once the PII is received by US-VISIT, existing US-VISIT privacy and security controls protect the information. The systems supporting US-VISIT are certified and accredited, and they are operated in accordance with US-VISIT and DHS policy and all applicable privacy and security regulations. These systems undergo periodic assessments of their physical, technical, and administrative controls to enhance accountability and data integrity. Obtaining access to the systems is controlled through documented procedures based on least privilege, need to know, and established job responsibilities. These procedures and access logs are subject to management oversight that confirms compliance with privacy and security requirements. All individuals with access to the systems receive mandatory security and privacy training relevant to their roles. Contractor personnel must also sign nondisclosure agreements. Detailed rules of behavior have also been developed to support the users acting within the systems.

Moreover, US-VISIT mitigates the risk of unauthorized individuals obtaining access to PII in transmission by using a secured telecommunications line that complies with standards set forth in the ISAs. These ISAs are required to be executed prior to external access to DHS systems to receive and transfer information in support of the DHS/UKBA International Group Visa Services project.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics, and other technology.



9.1 What type of project is the program or system?

The DHS/UKBA International Group Visa Services project is an operational project that uses US-VISIT systems to biometrically query UKBA International Group Visa Services applicants against the IDENT list of subjects of interest and to manage positive results through TRACS. These systems are composed of standard commercial technology and customized hardware and software required to meet the needs of US-VISIT.

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

US-VISIT uses the Enterprise Life Cycle Methodology (ELCM), which enables projects to follow a structured and repeatable process from initial concept through discrete business outcomes. The new connections between the systems supporting US-VISIT and UKBA International Group Visa Services are following the US-VISIT ELCM process. The US-VISIT systems are also managed by the ELCM process and are currently in the operations and maintenance phase.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

As proposed, US-VISIT support for the DHS/UKBA International Group Visa Services project relies on the same primary technologies that currently support US-VISIT. The technologies consist of standard electronic communications and data storage systems. The matching algorithms used by US-VISIT to biometrically verify and search the IDENT list of subjects of interest do not present specific privacy concerns and are developed in an environment subject to strict administrative, technical, and policy controls.

Given the sensitivity of the data and the need for a high degree of data integrity to ensure correct conclusions, US-VISIT has established an ELCM that embeds privacy risk assessment and documentation into project development. Technical and programmatic design choices are informed by this approach, such that proposed changes are assessed in terms of life-cycle processes—collection, use and disclosure, processing, and retention and destruction—and the potential they may create for noncompliance with relevant statutes or regulations (the Privacy Act in particular) or for violations of fair information principles. When analysis determines that privacy risks may exist, either alternative design choices or appropriate technical, physical, and/or procedural mitigations are developed.



Approval Signature Page

Original signed and on file with DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security