Privacy Impact Assessment
for the

US-VISIT Five Country Joint Enrollment and Information-Sharing Project (FCC)

November 2, 2009

Contact Point

Paul Hasson, Privacy Officer
US-VISIT Program
National Protection & Programs Directorate
(202) 298-5200

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

Abstract

The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program of the Department of Homeland Security (DHS) publishes this privacy impact assessment (PIA) to cover a new, systematic, and long-term information-sharing project with trusted partner nations for immigration purposes. The Five Country Conference (FCC) is a forum for co-operation on migration and border security, between the countries of Australia, Canada, New Zealand, United Kingdom, and the United States. The FCC Information-Sharing Project is a partnership among all the members of the FCC that is aligned with the DHS mission as well as the US-VISIT Strategic Plan because it will help identify individuals whose identities were previously unknown and by doing so, improve national security in support of DHS-wide initiatives and other mission goals.

Overview

The guiding principles of US-VISIT are to enhance the security of our citizens and visitors; facilitate legitimate travel and trade; ensure the integrity of the immigration system; and safeguard the personal privacy of visitors. US-VISIT provides biometric and biographic services to other DHS entities—including U.S. Customs and Border Protection, U.S. Coast Guard, U.S. Citizenship and Immigration Services, and U.S. Immigration and Customs Enforcement—to enable them to make better decisions about admissibility into the United States; and to assist other Federal, State, local, tribal, and foreign law enforcement agencies that support DHS in strengthening national security and in meeting law enforcement objectives.

Under the auspices of the FCC,US-VISIT is developing a new capability that supports immigration processes, including asylum and refugee determinations among the governments of the United States, Canada, the United Kingdom, Australia, and New Zealand (hereafter called FCC partners). This capability allows FCC partners, including the United States, to exchange biometric information in specific immigration cases where:

- the identity of the individual is unknown or uncertain;
- the individual's whereabouts are unknown; or
- there is reason to suspect that the person has been encountered by one of the countries participating in the Protocol.

The biometrics are exchanged to search against the existing biometric holdings of each FCC partner for determining the existence of information that may be pertinent to immigration and border management decision makers.

The FCC project aligns with the mission of US-VISIT to facilitate legitimate travel; to prevent immigration and identity fraud; to identify inadmissible individuals, individuals with outstanding wants or warrants, and those convicted of certain crimes; to identify those who are attempting to gain admission into or are seeking a benefit from an FCC country by fraud; and to resolve immigration and other cases requiring identity or confirmations of an individual's location.

An example of a standard FCC information exchange may include when there is reason to believe that an individual who is seeking an immigration benefit may have been previously encountered in another FCC country, a FCC "requesting country" will securely transmit the individual's biometric identifiers (such as fingerprints) to a FCC "providing country" for a system search. The providing country will make a best effort to respond within 72 hours to the requesting country with whether or not a biometric match was made, and if so, with the biographical and encounter information associated with the individual (if it is appropriate to share), enabling the requesting country to better determine whether the individual is lawfully

entitled to the immigration benefits he/she seeks. Other examples of the uses of the FCC project are outlined in Section 2.1 of this PIA.

Since the FCC project represents a move toward systematically exchanging information, this PIA is being published to describe the privacy and security safeguards in place for the project.

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 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?

Information collected, used, disseminated, and maintained may include biographic and biometric information. Biometric information may include fingerprints and digital facial photographs, and the reason and date the biometric was collected. Biographic information may include 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, and country of issuance), current whereabouts (if known), and gender.

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

Information may be collected by various means. Within DHS, information in the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program is collected directly from individuals by other DHS agencies and from external organizations such as the Department of State, foreign government border management agencies, and other designated entities that collaborate with DHS in pursuing national security, law enforcement, immigration, intelligence, and other functions related to the DHS mission. Additionally, if US-VISIT is alerted to a match by a providing country, the facts regarding the match if it is relevant and appropriate may be retained.

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

Information exchanged in the FCC project is collected, used, and disseminated to facilitate and enhance the quality and timeliness of immigration and admissibility decisions; to prevent immigration and identity fraud; to identify inadmissible individuals, individuals with outstanding wants or warrants, and those convicted of certain crimes; to identify those who are attempting to gain admission into or are seeking a benefit from an FCC country by fraud; and to resolve immigration and other cases requiring identity or confirmations of an individual's location.

1.4 How is the information collected?

The FCC project is an information exchange effort among partnering countries that uses existing biometric holdings. In the United States, the information that US-VISIT maintains is generally collected

electronically at the time an individual visits a U.S. government (or government-sponsored) location to submit an application for a visa or entry to the United States; during an initial in-person screening at a U.S. embassy/consulate or port of entry into the United States; or during an encounter with a designated entity collaborating with DHS in pursuing national security, law enforcement, immigration, intelligence, or other functions related to the DHS mission. All information collections are performed in strict compliance with the appropriate legal, policy, business, and privacy/security requirements that govern the particular information collection environment, and only the minimal amount of information necessary is collected.

1.5 How will the information be checked for accuracy?

US-VISIT information is checked for accuracy through multiple quality reviews to ensure a minimum level of completeness and quality. Initial quality reviews are conducted by comparing against the submitted documentation, such as an identification card, passport, or other corroborating documentation; and if necessary by conducting an in-person interview. An individual is also provided the opportunity to correct or amend information if he or she believes the information is not accurate. (Additional information is available in section 7.2 of this PIA.) Additionally, FCC partners are authorized to request subsequent corrections, changes, and deletions when necessary and appropriate. Finally, robust multilateral administrative policies ensure that inaccurate information is detected and corrected in a timely manner. Each FCC country is responsible for its own information; and to ensure that no one is harmed by inaccurate information held by another FCC country, each FCC country must provide individuals with access and redress**.**

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

The specific legal authorities, arrangements, and agreements that allow US-VISIT to engage in the collection and sharing of information for the FCC project include, among others, the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (Pub. L. 104-208); the Data Management Improvement Act of 2000 (Pub. L. 106-215); the Enhanced Border Security and Visa Entry Reform Act of 2002 (Pub. L. 107-173); the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-458); and Implementing the Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110-53). In addition, there are formally signed bilateral international data-sharing protocol documents and memoranda of understanding (MOUs) between DHS and each FCC partner.

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

Privacy risks identified are mitigated using a variety of approaches. US-VISIT analyzed and conducted comprehensive reviews of perceived risks related to sharing information. All FCC partners are confident that the appropriate safeguards for information protection are addressed. Each FCC partner formally signed a bilateral international data-sharing protocol document and a MOU that specifies the numerous protocols framing the sharing agreement. These protocols, MOUs, and sharing agreements include numerous privacy and security safeguards. Examples of FCC privacy and security protocols are:

- System queries are performed on biometric information only (instead of name-based queries).

- Security controls are established before implementation and are reviewed annually.
- Project and security controls are subject to rigorous testing.
- Only authorized users with an absolute need-to-know are granted access.
- Personal information is exchanged using a two-factor authentication methodology requiring file encryption.
- Biometric information without a match is destroyed promptly after searching is completed.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

Information shared in the FCC project is used by a FCC Country for immigration and border management, national security, and law enforcement purposes in that country only. Uses may include, but are not limited to, the following immigration situations:

- Where there is an indication of derogatory activity (e.g., child smuggling) or other associations of concern such that the individual could be found inadmissible to one or more of the FCC partner countries.
- Where the identity of the individual is unknown (e.g., an individual who has destroyed his or her identifying documents or withheld information about his or her identity to prevent removal).
- Where there is reason to believe that another FCC partner has encountered the individual.
- Where there is an asylum claim that involves identifying individual(s) encountered inside the FCC partner country, or locating individuals whose whereabouts are unknown or who may have violated immigration or criminal laws.
- Where an individual requires re-documentation for removal or another immigration-related process.

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

To assist in trend analyses, investigations, and the management of cases in support of controlling illegal immigration, eliminating fraud, determining fraud and encounters, and other law enforcement/investigative uses, system tools may be used for producing management or statistical reports, e.g., total number of requests made (by country), number of matches made, reason for request, result of follow-up action, and amount of time to return results.

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

The FCC project does not use commercial or publicly available information.

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 ensure that information is handled in accordance with appropriately defined and authorized uses, each FCC partner adheres to a formally signed bilateral international data-sharing protocol document and an MOU or annex that includes strict privacy and security safeguards and controls. In addition, the DHS Chief Privacy Officer exercises oversight to ensure that information is properly protected in accordance with current U.S. privacy laws and DHS guidance on confidentiality and the integrity of personal information. In addition, the US-VISIT Privacy Officer ensures that information is collected, used, accessed, and maintained appropriately, and that all appropriate physical, electronic, and procedural safeguards are implemented to protect the information against loss, theft, or misuse, as well as unauthorized access, disclosure, copying, use, modification, or deletion. Examples of some of the controls that all FCC partners agreed to implement are:

- An agreement that classified information will not be exchanged.
- A two-factor authentication methodology for accessing information.
- A protocol for verifying that only authorized personnel with an official need to know have access to information.
- Any information modification (i.e., additions, changes, deletion, retention, and destruction or return) is carefully tracked and logged.

Section 3.0 Retention

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

3.1 What information is retained?

All shared biometric information is generally destroyed as soon as the receiving country has completed searching (whether or not a match is achieved), and is not used for any other purpose. When there is a legitimate purpose connected with a match, an FCC partner may store, process, and transmit further biometric and biographical information, in accordance with applicable laws and established information retention policies. Additionally, if US-VISIT is alerted to a match by a providing country, the facts regarding the match if it is relevant and appropriate may be retained.

3.2 How long is information retained?

Unless otherwise prohibited, all FCC information is destroyed in a timely manner after searching is completed. However, when there is a legitimate purpose connected with a match, an FCC partner may store, process, and transmit further biometric and biographical information, in accordance with applicable laws and established information retention policies. According to MOU 2.12, the Providing Participant is expected to destroy the fingerprints in a secure manner and use them for no other purpose once the search against its relevant biometric systems is complete. NARA has authorized US-VISIT to retain information for 75 years from the date of admission into the U.S. in order to ensure that the information related to a particular border crossing is available for providing any applicable benefits related to immigration or for other law enforcement purposes.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

The US-VISIT record retention schedule of 75 years has been approved by the National Archives and Records Administration and is in accordance with published DHS record schedules.

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

Ensuring that information is retained for only the minimum amount of time necessary reduces the risks associated with maintaining information for a longer time. All information exchanged between FCC partner countries is destroyed timely as specified in the MOU or annex, unless there is a match and a legitimate purpose for retaining the information. Finally, audit schedules require verification that all FCC partners comply with applicable information retention schedules.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within DHS.

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

US-VISIT may share FCC information internally with any DHS entity with which it has a formal information-sharing agreement, for the purpose of maintaining secure borders, immigration management, and identity verification. The shared information may include fingerprints, digital facial images, date and reason biometrics were collected, 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, and country of issuance), current and historic whereabouts of the individual, and gender.

4.2 How is the information transmitted or disclosed?

US-VISIT electronically transmits FCC information within DHS using existing DHS networks, technology, systems, processes, and facilities.

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.

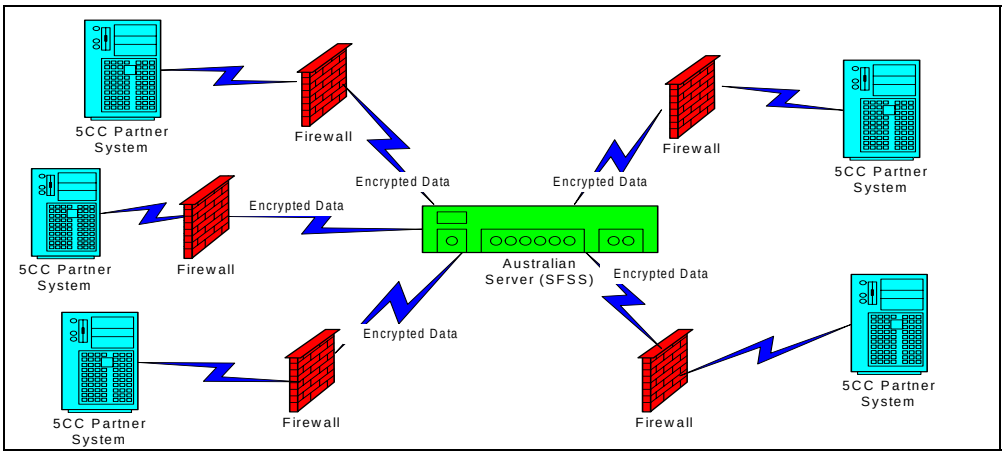
As specified in the bilateral international data-sharing protocol document and MOU or annex, internal information sharing within DHS is authorized. A risk may exist that information could be shared for a purpose other than that defined by the FCC protocol document, but that risk is mitigated by training and awareness of appropriate uses.

Section 5.0 External Sharing and Disclosure

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

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

US-VISIT information is shared externally with the FCC partners for the purposes of maintaining secure borders and preserving the integrity of the immigration systems of participating governments. The FCC information that is shared may include fingerprints, digital facial photographs, date and reason the biometrics were collected, 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, and country of issuance), current and historic whereabouts, and gender. In the event of an information match, two FCC partners (the requesting and providing countries) may further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether further action is required using other existing protocols (law enforcement or otherwise) between the countries. Information received by any FCC partner is to be used in determining the handling of an immigration case in that country only. FCC partners do not share information exchanged under this protocol with non-FCC partners without the permission of the FCC partner(s) that originally provided the information. For search requests resulting in matches against two or more countries, information may only be exchanged initially on a bilateral basis; however, the requesting country may inform each providing country about the existence of another matching record and the identify of the other FCC partner(s) with a matched record. The illustration below demonstrates how information is shared between FCC partners.



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 personally identifiable information outside of DHS is compatible with the original collection of that information and is covered by the appropriate system of records notice (SORN) and PIA, including this PIA. To view all the PIAs and SORNs for DHS and the US-VISIT program, visit www.dhs.gov/privacy. Other FCC partners are subject to their respective laws, regulations, and policies relating to the exchange and maintenance of personally identifiable information.

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

All information sent outside of DHS must comply with strict security measures that safeguard its transmission. All FCC partners have agreed to implement these security standards, including implementing a two-factor authentication requirement whenever information is removed from, or accessed from outside, the agency.

For authentication assurance, searching requests are transferred using a two-factor authentication method that then prompts an automatic notification to the providing country. Each FCC partner accesses the transfer file and retrieves the information for searching against its biometric immigration information holdings. Information is returned in a similar fashion. In the event that the standard method for sharing information is unavailable, the first contingency for transferring between the requesting country and the providing country is direct country-to-country communication using advanced encryption standards. Finally, in the unlikely event that both methods are unavailable and the request is of a critical nature, the second contingency for information transfers is using the secure networks of FCC embassies or high commissions, and then hand-delivering the encrypted results to the appropriate agency in the providing country.

Additionally, US-VISIT's Information Systems Security Team ensures strict compliance with policies and rules governing the exchange of information and implements appropriate transaction and business logic and rules to ensure that searches and match results are in accordance with agreed-upon policies and business and security frameworks within the FCC project and the technical environment for DHS.

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

Considering the extent of external information sharing, an identified privacy risk is that information could be shared outside of the two exchanging countries without appropriate authorization or for a purpose other than that originally defined. To mitigate this risk, the FCC protocol requires that any disclosure of information be between the applicable FCC partners for the stated purposes specified in the MOU or annex. Additionally, a project manager ensures that all aspects of the MOU or annex are being followed and that access to information exchanged under the project is allowed only to authorized personnel with a need to know. Audit schedules require verification that all agreed-upon protocols are being followed. The DHS Chief Privacy Officer exercises oversight of DHS activities to confirm that information systems are fully compliant with current privacy laws and guidance, and the US-VISIT Privacy Officer ensures that projects and systems are operating within the established guiding principles of the program. Finally, in the event of a situation that disrupts a normal transfer of information, an FCC partner project manager must immediately notify the other FCC partners by telephone or e-mail.

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 of the sharing of FCC information is provided by the publication of this PIA.

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

Individuals have the right to decline to provide information during the application or arrival period; however, declining to provide information could result in an adverse action, such as a determination of inadmissibility to the United States.

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 and/or their parents, sponsors, or representing attorneys/agents do not have the right to consent to particular uses of the information. Information is provided voluntarily without the expectation of a right to limit the use of the information, consistent with all disclosed purposes and uses.

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.

Notice is provided to individuals by various means, such as by the inclusion of a privacy notice on information collection forms/applications or on posters/banners displayed at international arrival ports of entry. To further ensure awareness, additional disclosure is provided by this PIA and other publicly posted US-VISIT PIAs and SORNs in the Federal Register. PIAs and SORNs are also posted on the DHS public-facing Web site. To view all PIAs and SORNs for DHS and US-VISIT, as well as to learn more about DHS privacy programs, visit www.dhs.gov/privacy and follow the links.

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?

In accordance with the provisions of the Privacy Act of 1974 and the Freedom of Information Act (FOIA), the procedures that allow individuals to gain access to information in a DHS system of record are posted on the DHS public-facing Web site: http://www.dhs.gov/index.shtm. Individuals may request access by contacting: US-VISIT Privacy Officer, Department of Homeland Security, 245 Murray Drive, SW., Washington, DC 20598-0675. Requests for information are evaluated to ensure that the release of information is lawful; will not impede an investigation of an actual or potential criminal, civil, or regulatory violation; and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

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

The procedures for correcting inaccurate or erroneous information maintained by US-VISIT are available by visiting the DHS Traveler Redress Inquiry Program (DHS TRIP) on the DHS public-facing Web site: http://www.dhs.gov/index.shtm. Individuals may also submit a redress request by contacting: US-VISIT Privacy Officer, Department of Homeland Security, 245 Murray Drive, SW., Washington, DC 20598-0675.

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

Individuals are advised of the procedures for correcting their information via the DHS public-facing Web site (http://www.dhs.gov/index.shtm) or by contacting the US-VISIT Privacy Officer, Department of Homeland Security, 245 Murray Drive, SW., Washington, DC 20598-0675.

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

Formal redress is provided. In addition, if an individual is dissatisfied with the response to his or her redress inquiry, he or she may appeal to the DHS Chief Privacy Officer, who reviews the appeal and provides final adjudication concerning the matter. The DHS Chief Privacy Officer may be contacted at Chief Privacy Officer, Attn: US-VISIT Appeal, Department of Homeland Security, Washington, DC 20528, USA; or by fax: 1-202-772-5036.

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

The FCC project benefits from a minimal privacy risk associated with redress due to DHS TRIP serving as a single point of contact for individuals requesting resolution to a travel issue related to DHS. US-VISIT encourages the use of TRIP as a central point of redress, so that if a person has issues with more than one component, they can be addressed and resolved concurrently by the different components reducing the total time to correct his record. If erroneous information is determined to exist, DHS and all FCC partner countries apply the appropriate changes, deletions, or corrections and notify one another when corrective action should be taken.

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?

Documented procedures determine which users may access the information. As specified in the MOU or annex, access to information is strictly limited to those authorized FCC partner personnel who have a need to know for official duties. Each FCC partner has an administrator responsible for granting access to registered users and for maintaining and updating a comprehensive list of registered users. At DHS, before a unique user account for access to FCC information is assigned, users must have authorized access to the DHS network. A signed user access agreement requires supervisor certification that access is needed for official duties. DHS user access agreements also include rules of behavior regarding responsibilities for safeguarding personal information and the consequences and accountability for violating these responsibilities. At US-VISIT, completed user access agreements are reviewed and approved by the US-VISIT Information System Security Officer (ISSO), who reviews and approves completed user access agreements before unique user accounts are assigned.

8.2 Will Department contractors have access to the system?

Access to FCC information is given to authorized DHS contractors with security clearances and a justified need to know.

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

DHS provides comprehensive privacy training to all DHS personnel prior to assigning access to the DHS unclassified network. Additionally, US-VISIT provides its staff with specific privacy training and annual refresher or role-based training. All DHS and US-VISIT system users must complete annual refresher training to retain system access. Privacy training for the other FCC partner participants is in accordance with the appropriate training requirements defined in the technical environment for each FCC partner.

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

US-VISIT information systems that support the FCC project are all certified and accredited. Certification and accreditation for systems maintained by other FCC partners is in accordance with the appropriate business and security requirements defined in the technical environment.

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

DHS has well-established and comprehensive processes that enhance information security and minimize possibilities for misuse or abuse. The FCC project adheres to all of these internal information security policies, as outlined in the DHS information technology security documents, and will be periodically audited and evaluated to ensure continued compliance with DHS security requirements. A formal bilateral international data-sharing document in addition to the MOUs (between DHS and each of the other FCC Partners) or annex will define the auditing measures and technical safeguards that other FCC partners agree to employ, in addition to providing the appropriate business and security requirements defined in the technical environment.

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?

To address the privacy risks associated with the sensitivity and scope of the FCC project, a variety of security controls have been implemented. FCC information is protected by strict administrative, technical, and physical safeguards appropriate to the sensitivity of the information. For example, the FCC project uses encryption and two-factor authentication. Users with authorized access are registered and then serve as points of contact for searching requests for their respective countries. Each FCC partner is responsible for maintaining and updating a comprehensive list of registered and approved users. The FCC project operates in accordance with required DHS and Federal information security requirements and policies to ensure that information is appropriately safeguarded, and complies with any other applicable business and security requirements defined in the technical environment for each FCC partner.

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 FCC project is a systematic, long-term, information-sharing project that supports better determinations of identity, immigration status, and immigration process using existing technologies, systems, and processes to facilitate biometric-searching requests via US-VISIT. To view the PIA for US-VISIT, visit www.dhs.gov/privacy and follow the link to "Privacy Impact Assessments."

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

The FCC project is in the early stage of development. A controlled and limited pilot was completed and, based on an analysis of the pilot, the FCC project is implementing the systematic solution described in this PIA. If the FCC project undergoes a significant modification, or expands its scope, an updated PIA will be conducted.

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

In addition to employing existing technology, systems, processes, and facilities, the FCC project employs a central secure file share server (SFSS) operated by the Australian Department of Immigration and Citizenship (DIAC) that is unique to this project. The illustration in section 5.1 demonstrates how the SFSS exchanges information.

To address any privacy concerns, all FCC partners are responsible for protecting information behind their respective firewalls, up to and including when information is uploaded to the SFSS. As the SFSS owner, the Government of Australia is responsible for protecting the information residing on the SFSS, as well as for providing availability to the SFSS and monitoring/reporting activities conducted on the SFSS. All FCC partners agree to comply with these and other security and technical requirements specified in the formally signed bilateral international data sharing protocol document and MOU or annex. Information exchanges may be suspended if legal or privacy policy issues or differences are identified. Information exchanges may resume only after all issues/differences are addressed, resolved, or reconciled. Each FCC partner imposes appropriate business logic/rules to ensure that searches and match results are in accordance with agreed upon technical, legal, policy, business, and security frameworks within their respective environments.

Responsible Official

Paul Hasson
US-VISIT Privacy Officer
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security