Privacy Impact Assessment
for the

United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program

Comprehensive Exit Program: Air Exit Pilot

May 20, 2009

Contact Point
Paul Hasson
Privacy Officer
US-VISIT Program
(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 is implementing a new pilot phase of a comprehensive exit program for integrating non-U.S. citizen departure with existing arrival information. The Exit Program requires the collection of minimal biometric and biographic data from covered aliens, enabling US-VISIT Entry/Exit matching, identity verification, and cross-checking against a list of subjects of interest. This Privacy Impact Assessment (PIA) is conducted because US-VISIT collects personally identifiable information on non-U.S. citizens.

Overview

The Department of Homeland Security (DHS) created the US-VISIT Program to implement a biometric entry and exit system. In 2004, US-VISIT took its first step toward meeting this objective by deploying biometric collection capabilities at ports of entry (POEs) concurrent with the deployment by the Department of State of biometric collection capabilities at visa-issuing posts. The records stored by US-VISIT are primarily composed of data about foreign nationals who have legally entered or applied to enter the United States. As the system owner of these records, US-VISIT is in a unique position to biometrically identify people with unprecedented accuracy and to provide authorized officials with information about these individuals that might warrant further action. US-VISIT's capabilities support a broad range of Federal, State, and local government agencies that make a variety of risk and eligibility decisions related to the issuance of visas; admissibility to the United States (U.S.); adjudication of immigration benefits; matters of national security; law enforcement actions; intelligence and trend analysis; and the issuance of credentials (i.e., determining if an individual should be granted access to a critical facility or sensitive system). Through such collaboration, US-VISIT seeks to close gaps that allow criminals, potential terrorists, or other persons of interest to enter our Nation undetected.

The US-VISIT Program has been implemented in phases, with each phase adding improved capabilities. US-VISIT will first focus on implementing biometric exit collection at airports and then address deployment at land and sea POEs. This PIA addresses "Air Exit," a new pilot phase of a comprehensive exit program for integrating non-U.S. citizen departure information with existing arrival information. The Air Exit pilot is being conducted at the Detroit Metropolitan Wayne County (DTW) and Atlanta Hartsfield-Jackson (ATL) airports (subject to change). U.S. Customs and Border Protection (CBP) and U.S. Transportation Security Administration (TSA) participation in the pilot is limited to facilitating the collection of limited biometric and biographic information from certain "in-scope" travelers on behalf of US-VISIT during the Air Exit pilot. In-scope travelers are generally defined as non-U.S. citizen visitors, including Lawful Permanent Residents (LPRs), between the ages of 14 and 79 with the exception of certain Canadian and Mexican citizens and visitors subject to National Security Entry-Exit Registration System (NSEERS) registration or admitted on certain visas (hereafter referred to as "non-U.S. citizen visitors"). [1]

The purpose of the pilot is to evaluate the impact of collecting biographic and biometric information at departure gates and TSA security checkpoints. Certain non-U.S. citizen visitors with an international destination are directed to areas near the departure gate or at the TSA checkpoint for biographic and biometric information collection. Using a mobile or portable collection device, the officers collect one or more electronic fingerprint(s),[2] and the associated biographic information that is contained

[1] Additional information about LPR and non-U.S. citizen visitor entry and exit requirements is available in the Final Rule (73 FR 77473) and the *Enrollment of Additional Aliens in US-VISIT* Privacy Impact Assessment at http://www.dhs.gov/privacy.

[2] The collection standard for this pilot has evolved from requiring as many as ten (10) prints to as few as one (1) from each hand. At present, the officers will collect two (2) prints from the right hand.

on a Machine Readable Travel Document (MRTD), such as name, date of birth, document issuance type, country, and number.

The Consolidated Security, Disaster Assistance, and Continuing Appropriations Act of 2009, Pub. L. 110-329, Div. D (2009 Appropriations Act) calls for a commercial air carrier to participate in the Air Exit pilot and facilitate the collection of biometric data from non-U.S. citizen visitors departing the United States. Because no air carrier agreed to participate, US-VISIT submitted a request to National Protection and Programs Directorate (NPPD) to proceed with the implementation of one air biometric pilot with CBP and one air biometric pilot with TSA. On March 23, 2009, NPPD approved this request to proceed with the pilot without air carrier participation.

The portable and/or handheld biometric and biographic collection devices verify the clarity and machine-readability of the data collected. Data is encrypted as it is collected. At both the Atlanta and the Detroit airport locations, the biometric and biographic data are transmitted in an encrypted format to a secure, dedicated DHS notebook computer and then to the US-VISIT IDENT system. The data remains encrypted during the entire transmission process. And the data is automatically deleted from the mobile device and DHS notebook computer after each step of the transmission process is completed. To minimize the potential for theft or loss, the devices and DHS notebook computers remain in the control of CBP or TSA at all times. When not in use, the mobile devices and DHS notebook computers are stored at secure CBP and TSA offices at the respective airport locations. To minimize other privacy concerns, the mobile devices and DHS notebook computers incorporate strict physical and procedural controls, FIPS-compliant data encryption, residual information removal, and require authorized users to sign in using account names and passwords.

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?

The personally identifiable information (PII) that is collected, used, disseminated, and maintained for this Air Exit pilot includes: fingerprint images, 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), and gender.

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

The sources of the information for Air Exit are certain non-U.S. citizen visitors departing the United States from Detroit Metropolitan Wayne County (DTW) and Atlanta Hartsfield-Jackson (ATL) airports (subject to change). On behalf of US-VISIT, CBP is facilitating the collection of information at DTW, and TSA is facilitating the collection of information at ATL.

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

In addition to evaluating the impact of collecting biometric and biographic information at departure gates and TSA checkpoints, information is collected, used, disseminated, and maintained to verify identity; conduct terrorist, criminal, and immigration violation checks; and integrate arrival and departure information for the purposes of immigration and border management, national security, and law enforcement.[3] As required by the Department of Homeland Security Act Appropriations of 2009, US-VISIT biometrically verifies the identity of previously encountered non-U.S. citizen visitors departing the United States. US-VISIT also conducts biometric checks against a list of subjects of interest. Results of these biometric checks are referred to and managed by the appropriate DHS agencies on a case by case basis. Biometrics that match a non-U.S. citizen visitor's US-VISIT record are associated with that record and stored in the US-VISIT Automated Biometric Identification System (IDENT). When the identity of a non-U.S. citizen visitor cannot be biometrically verified against a previous encounter, the biometric is stored in IDENT but is not associated with a previously collected IDENT record. The IDENT PIA is available at: http://www.dhs.gov/privacy.

1.4 How is the information collected?

CBP Officers and TSA Security Officers (TSOs) facilitate the collection of biometric and biographic information using a briefcase and/or handheld biometric and biographic collection device. Certain non-U.S. citizen visitors with an international destination are directed to areas near the departure gate or by TSOs at the TSA checkpoint for biometric and biographic information collection. The collection devices scan fingerprint data and Machine Readable Travel Documents (MRTD), such as passports and visa documents.

CBP uses temporary signage at the gate for a flight identified for participation in the Pilot. The signage directs non-U.S. citizen visitors as to the procedures for complying with the program (e.g., where to line up, which fingers to present for scanning, etc.). CBP Officers, acting on behalf of US-VISIT, collect biographic information from the MRTD using the mobile collection device. After confirmation that the individual is in-scope, the CBP Officer facilitates the collection of biometrics.

TSA determines in-scope individuals by reviewing the presented form of identification and the destination indicated on the boarding pass. If the individual is initially determined to be in-scope, the individual is directed to the biographic/biometric collection area. The TSO, acting on behalf of US-VISIT, will swipe the MRTD through the mobile collection device to collect biographic information. Based on the biographics, these devices are capable of alerting the officers as to whether the individual is in-scope or out-of-scope. [4] After confirmation that the individual is in-scope, the TSO facilitates the collection of biometrics. After the TSO has completed the information collection, the individual is escorted to the TSA screening checkpoint.

1.5 How will the information be checked for accuracy?

Multiple quality checks are performed on the biometric and biographic information to ensure the information meets a minimum level of completeness and quality. Quality checks are conducted against the submitted documentation by verifying the information provided against a passport and/or another

[3] These actions are back-end processes that occur after the data has been transmitted to DHS servers.
[4] If the individual is not in-scope, the TSO will delete that individual's biographics from the mobile device, and the individual will be escorted to the TSA screening checkpoint.

corroborating document, and if deemed necessary, by an in-person interview. Accuracy is also enhanced by providing individuals the opportunity to amend information if it is determined to be erroneous (additional information is available in Section 7.2 of this PIA). Finally, robust multi-lateral administrative policies ensure that inaccurate information is detected and corrected in a timely manner.

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

In addition to the legal authorities that oversee implementation of US-VISIT, the legal authorities, arrangements, and agreements that specifically define the collection of Air Exit information are found in the Secure Travel and Counterterrorism Partnership Act of 2007 (STCPA). The STCPA directs the Secretary of DHS to establish an exit system that records the departure information of non-U.S. citizen visitors to the United States.

The Consolidated Security, Disaster Assistance, and Continuing Appropriations Act of 2009, Div. D (Department of Homeland Security Act Appropriations, 2009) directs US-VISIT to implement a pilot where limited biometric and biographic data is collected from non-U.S. citizen visitors departing the United States by air.

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law 104-208, authorized the creation of an entry-exit system that integrates non-U.S. citizen visitor arrival and departure information. The Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA) requires the entry-exit system integrate all authorized or required arrival and departure data in electronic format.

The Visa Waiver Permanent Program Act, Section 205 (October 30, 2000), provides for the creation of a system that contains a record of the arrival and departure of every non-U.S. citizen visitor admitted under the Visa Waiver Program at air or sea ports of entry. The provisions of the DMIA subsequently resulted in the integration of the Visa Waiver Program arrival/departure information into the primary entry-exit system component of US-VISIT.

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

Potential threats and privacy risks include collecting data from out-of-scope travelers, possible subsequent denial of admission to the United States based on faulty data, or misuse of PII. DHS seeks to address these risks by minimizing the collection and transmission of PII where possible. CBP Officers and TSOs use the biographic scanning devices to help determine if the traveler is in-scope. One or more electronic fingerprint(s), and a limited amount of associated biographic information that is contained on a Machine Readable Travel Document (MRTD), such as name, date of birth, document issuance type, country, and number is collected.

Collecting fingerprint data is necessary to meet the biometric requirements placed on the US-VISIT Program by statute. Collecting biographic information is necessary to facilitate the biometric identity verification and biometric check against DHS lists of subjects of interest. DHS protects the PII collected through robust privacy and security policies, procedures and standards governing data collection and use.

Redress procedures are discussed in Section 7.0. Security and technology risks and mitigation strategies for the mobile and handheld biometric collection devices are discussed in Sections 8.0 and 9.0.

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.

US-VISIT stores and uses the data collected during the Air Exit process to record the departure of non-U.S. citizen visitors, conduct certain terrorist, criminal, and immigration checks on lists of subjects of interest on covered aliens, and compare biometric identifiers to those collected on previous encounters to verify identity. The information collected assists other DHS entities such as CBP, U.S. Immigration and Customs Enforcement (ICE), and U.S. Citizenship and Immigration Services (CIS) to make better U.S. border and immigration management decisions. The information also assists other Federal, State, local, tribal, and foreign law enforcement agencies engaged with DHS in strengthening national security and meeting law enforcement objectives.

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

Air Exit relies on the same tools that currently support US-VISIT to analyze data for law enforcement purposes as well as intelligence and trend analysis, and quality assurance purposes critical for assessing risks related to border and immigration management operations.

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

Commercial or publicly available data are used only when needed to confirm previously collected information and/or to identify the address or telephone number of a non-U.S. citizen visitor after the data is transmitted to IDENT.

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.

Technical, security, and privacy requirements are in place for the devices that capture and transmit biographic and biometric information. CBP and TSA personnel are given privacy and security training related to collecting the information. Information is transmitted over an approved, encrypted DHS network that includes audit trail capabilities to monitor, log, and analyze system transactions as well as actions and system users' accesses. All audit records are managed per applicable DHS and/or US-VISIT official record schedules and record management procedures. In addition, all information is protected against unauthorized use, modification, and/or retention by a robust privacy and security program. US-VISIT records are protected consistent with all applicable privacy laws and regulations, including the publicly published US-VISIT privacy policy. Physical, technical, and administrative controls, which include access

controls and system user education and training, assist in keeping information secure and confidential. A program-dedicated privacy officer is responsible for overseeing compliance and ensuring that information is used appropriately.

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?

Air Exit information is retained by US-VISIT in accordance with the approved IDENT retention schedule of 75 years. The IDENT PIA is available at: http://www.dhs.gov/privacy.

Data stored on the mobile device is no longer needed once it is loaded into IDENT and is immediately deleted from the device upon confirmation of its successful transfer to the IDENT system.

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

Yes, the retention schedule has been approved by the component records officer and 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.

The risk associated with the length of time Air Exit information is retained is that the information may become vulnerable to unauthorized use or disclosure. To mitigate this risk, only the minimum amount of biometric and biographic data necessary to facilitate identity verification is collected. DHS will retain the PII in accordance with the NARA-approved retention schedule. Strict internal controls and auditing requirements are in place to guard against unauthorized use or disclosure.

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?

Information may be shared on a need to know basis in the performance of official duties with those DHS components engaged in border management, immigration enforcement, counter-terrorism, law enforcement, or national security. The sharing activities are consistent with data sharing and internal disclosures previously established for US-VISIT.

4.2 How is the information transmitted or disclosed?

Information may be shared via secured, encrypted networks. Any transmission or disclosure of information is done in accordance with a Letter of Intent (LOI), a Standard Operating Procedure (SOP), Interconnect Security Agreement (ISA), or data sharing agreements between US-VISIT and the respective data sharing partners.

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.

Potential risks and vulnerabilities are mitigated by partnering closely with all sharing organizations and implementing and documenting stringent operating procedures. DHS components are required to comply with the Department security policies and procedures, including the DHS Information Technology (IT) Security Program Handbook for Sensitive Systems. The handbook is a comprehensive guide that provides complete information security requirements to safeguard personal information. The guide also mandates roles and responsibilities, management policies, operational policies, technical controls, and application rules, to be applied to component systems, communications between component systems, and all interfaces between component systems. All DHS systems are fully secured, certified, and accredited. Information is shared on a need to know basis in the performance of official duties.

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?

Information may be shared with Federal, State, local, foreign, or tribal law enforcement agencies that, in accordance with their responsibilities, are lawfully engaged with DHS in strengthening national security and meeting law enforcement objectives.

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 System of Record Notice (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.

Personally identifiable information (PII) shared outside of DHS is compatible with the original purpose of collection. Sharing of PII is covered by the IDENT System of Records Notice (SORN).[5] DHS has established formal sharing agreements with non-DHS organizations which stipulate the narrow conditions for appropriate sharing or disclosure, including how the information must be protected and used, and how it must be aligned with a DHS mission. PII may be shared outside of DHS with appropriate Federal, State, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest, for purposes related to administering or enforcing the law, national security, immigration, or intelligence, where consistent with a DHS mission-related function as determined by DHS.

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

Information is shared outside of DHS in accordance with the IDENT SORN[6] for US-VISIT. When authorized, US-VISIT data may be shared using dedicated, secured networks, encrypted mobile devices, and secure connections. Any external transmission or disclosure outside of DHS must be in accordance with a formal agreement that contains binding transmission and security requirements.

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

The privacy risk is PII may be shared or used in a manner which is beyond the scope of the IDENT SORN or sharing agreement(s). This risk is mitigated by requiring sharing partners to implement secure standard operating procedures. These procedures are documented in binding Information Sharing Agreements (ISA). The ISAs establish a strict program designed to protect the confidentiality, integrity, and availability of shared information. DHS privacy and security programs require external sharing partners to establish and maintain strong rules of behavior for use of information, frequent periodic assessments and/or audits of physical, technical, and administrative controls, and regularly scheduled privacy/security training. US-VISIT contractors are required to follow the same privacy and security requirements as DHS staff.

---

[5] IDENT SORN, DHS/USVISIT-002, June 5, 2007, 72 FR 31080 < http://edocket.access.gpo.gov/2006/E6-11995.htm>

[6] Id.

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?

Non-U.S. citizen visitors receive notice regarding the collection of personally identifiable information through the IDENT SORN[7] publication in the Federal Register, a notice for the Collection of Alien Biometric Data upon Exit from the United States at Air Ports of Departure publication in the Federal Register, news conferences, media announcements, press releases, and this PIA. Banners and signs created by US-VISIT are posted at departure gates and at TSA security checkpoints provide notice to departing non-U.S. citizen visitors. The signage describes the requirement for non-U.S. citizen visitors departing the United States to provide biometric and biographic information and provides redress and contact information to address privacy concerns. US-VISIT also conducts ongoing outreach activities with commercial air carriers and travel agents. Commercial air carriers and travel agents can then inform and educate their clients on Air Exit biometric and biographic data collection requirements.

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

8 CFR Parts 214, 215 and 235, *Implementation of US–VISIT Biometric Requirements* states, "…the Secretary of Homeland Security or [her] delegate may require aliens to provide fingerprints, photographs or other biometric identifiers upon arrival in or departure from the United States." If a non-U.S.-citizen visitor fails to provide the requested biometric or biographic information, the individual may be deemed ineligible for future visas or admission to United States, or discretionary immigration benefits provided by 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?

When implemented, non-U.S. citizen visitors do not have the right to consent to particular uses of collected information. Information may be used for border and immigration management, national security, and law enforcement.

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.

US-VISIT conducts on-going public outreach and notice campaigns to increase awareness about information collection requirements. Federal Register publications, public announcements and outreach

[7] Id.

events, media releases, and publication of this PIA mitigate the risk that individuals may be unaware of collection requirements.

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?

The Freedom of Information Act (FOIA) and the Privacy Act allow individuals to gain access to their information. Specific information on how to do so is posted on the DHS public-facing website (http://www.dhs.gov/xfoia/editorial_0316.shtm) under "How to Submit a FOIA Request." The disclosure of some records or portions of a record may be subject to narrow exceptions for criminal or other law enforcement purposes. DHS extends access to all individuals, including U.S. and non-U.S. citizen visitors.

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

Inaccurate or erroneous information may be corrected using existing formal redress processes to correct information maintained by US-VISIT. Individuals may submit a redress request through the DHS Traveler Redress Inquiry Program (TRIP) website (https://trip.dhs.gov). Once a redress request is submitted, the request is reviewed, and the appropriate DHS entity is tasked to respond in a timely manner. When appropriate, inaccurate or erroneous information is corrected and the individual is notified of the resolution to his/her request.

Additionally, Privacy Act requests involving Air Exit information may be submitted to: US-VISIT Privacy Officer; Department of Homeland Security, Washington, D.C., 20528; Phone (202) 298-5200; Fax (202) 298-5201; US-VISIT-FOIA@dhs.gov.

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

Individuals are notified of the procedures for correcting their information through this PIA (as outlined above in section 7.2) and on the DHS public website. Additionally, redress procedures are published on the public facing DHS Traveler Redress Inquiry Program (TRIP) website, listed above.

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

Formal redress is provided. If an individual who uses the formal redress process is dissatisfied with the response received, he/she may appeal to the DHS Chief Privacy Officer, who will review the appeal and provide 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, D.C., 20528, USA; or Fax (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.

Inaccurate or erroneous information may cause inconvenience for non-U.S. citizen visitors attempting to re-enter the United States. If the data collected during exit does not match the data collected during entry, the next time the non-U.S. citizen visitor attempts to enter the U.S., CBP may send that individual to secondary screening in an attempt to resolve the mismatch problem. Non-U.S. citizen visitors will not be detained at the time of departure as a result of this pilot program.

A formal and robust redress process mitigates any privacy risks associated with Air Exit redress. The DHS TRIP website, referenced above, is an easy-to-use resource that serves as a central point-of-contact for the submission and processing of redress requests. Information is verified for accuracy through the performance of multiple quality checks. Quality checks are conducted against the submitted documentation to corroborate information, and, if necessary, personal interviews are conducted. Individuals may also request access to and/or a correction of their information, as permitted, pursuant to the FOIA or the Privacy Act.

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?

Air Exit utilizes strong documented operating procedures to determine which users may access information. Users accessing systems containing Air Exit information must hold appropriate security clearances, and complete mandatory security and privacy training, including annual refresher training, is required. Access is granted on the principle of least privilege, separation of duties, and need to know. A user's "need to know" depends on when, how, and why the user requires access to the information. Accordingly, "need to know" is asserted only after access has been established, and that assertion is validated and confirmed by the user's manager, the system manager, and security personnel. Each user is given a unique account name and password to access the device. Accurate event logs fully record all system access, and the Information System Security Manager (ISSM) confirms compliance with the 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 for DHS-owned systems, contractors may have access to the systems that support Air Exit, in performance of their official duties (such as system administration, monitoring, and security functions). Contractor access is granted in accordance with the principles of least privilege, separation of duties, and need to know. US-VISIT contractors may assist in the transmission of data from capture devices to US-VISIT systems. The access

policies and logs are reviewed by security management to ensure the effective implementation of privacy and security safeguards. Contractors are also required to possess appropriate security clearances, and complete mandatory security and privacy training.

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

CBP Officers and TSOs participating in the Air Exit Pilot receive special training that addresses privacy and security risks and requirements. All users of US-VISIT systems that support Air Exit receive mandatory privacy training. The training is specialized to address the unique privacy requirements of US-VISIT. DHS personnel, including government personnel and contractors, are required to take annual privacy refresher training offered by their respective DHS components. DHS personnel receive instruction on privacy regulations, legislation, responsibilities of the US-VISIT privacy program, and specific rules of behavior that may govern the operation of a particular system. Users external to DHS, who are a party to an information sharing arrangement, are also required to receive the same or similar privacy training, and annual refresher training in accordance with data sharing agreements.

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

Certification & Accreditation has been completed for the US-VISIT systems that support Air Exit.

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

Auditing measures and technical safeguards have been implemented to prevent misuse of information associated with the Air Exit pilot. These measures and safeguards are fully compliant with the requirements of DHS information technology security policy, in particular the DHS Information Technology (IT) Security Program Handbook for Sensitive Systems, which establishes a comprehensive protocol to ensure information security, in addition to directives on roles and responsibilities, managerial and operational policies, technical controls, and application rules. Audits are conducted to ensure continued compliance with DHS security requirements.

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?

Given the sensitivity and scope of the information, as well as the scope of the information sharing that is conducted, privacy risks are mitigated by DHS approving and employing the highest standards of technical, security, and privacy requirements. For example, to secure against unauthorized access, use, disclosure, or modification, the biometric data is encrypted upon collection. During the collection process, the agent conducting the collection of biometric data from in-scope travelers does not have access to this encrypted data. Technical and security measures are also enacted to prohibit the transmission of the encrypted biometric data from being forwarded to unintended third party recipients. In addition, existing

audit functions track all transmission and user activities related to the information, including access and modification once the data is transmitted to US-VISIT's systems. These procedures and access logs are subject to management oversight which confirms compliance with privacy and security requirements. The US-VISIT systems that support Air Exit are certified and accredited, and operate in accordance with strict DHS policies, and all applicable Federal privacy and security regulations. Systems undergo a periodic assessment of 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. All users with access to IDENT must possess security clearances, and take mandatory security and privacy training relevant to their responsibilities. CBP Officers and TSOs have successfully completed background investigations that include criminal checks, credit checks, and drug testing. Contractors and consultants must also sign non-disclosure agreements. Established, detailed rules of behavior are also in place for users accessing and supporting the systems.

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, radio frequency identification (RFID), biometrics, and other technology.

9.1 What type of project is the program or system?

The Air Exit pilot collects information from certain non-U.S. citizen visitors departing the United States. The information collected facilitates better border and immigration management through real time use of existing technology, systems, processes, and facilities.

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

Air Exit relies on existing, fully developed and implemented US-VISIT systems. To review all the PIAs for US-VISIT, visit http://www.dhs.gov/privacy and follow the link to "Privacy Impact Assessments."

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

Air Exit relies on the same forensic-quality digital fingerprint technology that currently supports US-VISIT. The deployable biometric technology used in Air Exit includes portable and/or handheld secure electronic communications and mobile data storage devices that incorporate strict access controls, precision, durability, and mobility. After the collection of biometric and biographic information, the devices provide real-time verification and encryption. The biometric and biographic data are transmitted in an encrypted format to a secure, dedicated DHS notebook computer and then to the US-VISIT IDENT system. The data remains encrypted during the entire transmission process. And the data is automatically deleted from the mobile device and DHS notebook computer after each step of the transmission process is completed. To minimize the potential for theft or loss, the devices and DHS notebook computers remain in the control of CBP or TSA at all times and when not in use are stored in secure locations (under the control of CBP or TSA). Additionally, to minimize other privacy concerns, the mobile devices and DHS notebook computers require strict physical and procedural controls, FIPS-compliant data encryption, residual

information removal, and built-in identification and authentication for all authorized users.

Responsible Official

Paul Hasson
Privacy Officer
US-VISIT
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