UPDATED

Privacy Impact Assessment for the

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

International Live Test – Phase II: Testing of ICAO-Compliant e-Passports from Selected Countries

December 22, 2005

Contact Point
Steve Yonkers, Privacy Officer
US-VISIT Program, DHS
(202) 298-5200

Reviewing Official
Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Summary of Update

This update to the Privacy Impact Assessment for US-VISIT addresses Phase II of the International Live Test. DHS evaluated the performance, both technically and operationally, of the e-Passports and reader solutions during Phase I of the International Live Test. The PIA for Phase I of the International Live Test was published in the Federal Register June 15, 2005. Phase II of the International Live Test will provide an opportunity to test basic access controls (BAC) of ICAO-compliant, international e-Passports against the selected U.S. document reader solution.

Introduction

The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program is an integrated, automated entry and exit capability that records the arrival and departure of aliens (defined as any person not a citizen or national of the United States); conducts certain terrorist and criminal checks on aliens; and verifies aliens' identities through comparison of biometric identifiers from a variety of systems. US-VISIT was established in response to a number of border protection and national security legal mandates and has the following primary goals:

- Enhance the security of our citizens and visitors;
- Facilitate legitimate travel and trade;
- Ensure the integrity of our immigration system; and
- Protect the privacy of our visitors

The US-VISIT Program is not a single system or database. Instead, it is a business process that integrates and enhances the capabilities of existing systems and permits interface with other Department of Homeland Security (DHS) and Department of State (DOS) systems, including: (1) the Arrival Departure Information System (ADIS), which currently stores summary information about alien travelers' arrivals, departures, and changes of status and matches these records to determine whether these travelers have maintained legal status or have illegally remained beyond their authorized period of stay; (2) a portion of the Automated Biometric Identification System (IDENT), which stores biometric records of aliens, including those travelers processed at the port of entry (POE) and visa issuance offices and facilitates identity verification and access to information in other biometric databases; (3) the Interagency Border Inspection System (IBIS), which is the passenger-processing component of the Treasury Enforcement Communication System (TECS), and which includes a lookout component, a primary crossing record archive, the Form I-94 Arrival/Departure Record repository, and an electronic manifest component, the Advance Passenger Information System (APIS), (4) the Automatic Identification Management System (AIDMS), which stores the Radio Frequency Identification (RFID) tag numbers associated with the Form I-94s; and (5) the Consolidated Consular Database (CCD), which belongs to the Department of State (DOS) and which stores biometric and biographic records of aliens who apply for visas. US-VISIT also interfaces with other DHS systems to facilitate transfer of information pertaining to changes or extensions in the status of individuals, including the Student and Exchange Visitor Information System (SEVIS) and the Computer Linked Application Information Management System (CLAIMS 3). SEVIS, which is managed by Immigration and Customs Enforcement (ICE), maintains information on international students and exchange visitors and

their dependents in F, M and J visa status in the United States, the schools that are DHS-certified to enroll international students, and the sponsors that are designated by DOS to host exchange visitors. CLAIMS 3 is the primary system used by the United States Citizenship and Immigration Service (USCIS) for the processing and administration of immigration benefits.

Consistent with guidance issued by the Office of Management and Budget (OMB) and policy guidance issued by the DHS Chief Privacy Officer, who has the statutory authority to require Privacy Impact Assessments (PIA) of proposed rules, this PIA for US-VISIT is being updated to reflect Phase II of the International Live Test which will test the ability to read biometrically-enabled travel documents compliant with International Civil Aviation Organization (ICAO) standards.

DHS evaluated the performance, both technically and operationally, of the e-Passports and reader solutions during Phase I of the International Live Test. The PIA for Phase I of the International Live Test was published in the Federal Register on June 15, 2005. Phase II of the International Live Test will provide an opportunity to test basic access controls (BAC) of ICAO-compliant, international e-Passports against the selected U.S. document reader solution.

During Phase II of the International Live Test, one U.S. Port of Entry (POE), San Francisco International Airport in San Francisco, California, and one international participant, Changi Airport in Singapore, will cooperate in the Live Test.

This activity necessitates a revision to this PIA to discuss the privacy risks. The US-VISIT PIA has also been revised to be consistent with internal DHS drafting guidance.

Section 1.0
Information collected and maintained

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

1.1 What information is to be collected?

Under the US-VISIT Program, the information to be collected from covered individuals consists of complete name, date of birth, gender, country of citizenship/nationality, passport number and country of issuance, country of residence, travel document type (e.g., visa), number, date and country of issuance, complete U.S. destination address, arrival and departure information, a digital photograph, digital fingerscans, and for travelers using land POEs after implementation of RFID, a unique and individually-assigned RFID tag number for each traveler. No new types of information will be collected under Phase II of the International Live Test. Table 1.3, in Section 1.3, lists the information and the purpose for which it is collected.

1.2 From whom is information collected?

Phase II International Live Test participants will be airline crew members and non-immigrants from Singapore, and diplomats and other officials from the U.S. This Live Test will take place from January 15, 2006, until April 15, 2006.

1.3 Why is the information being collected?

In numerous statutes, Congress has directed that an integrated biometric entry and exit program must be implemented for all aliens who enter or leave the United States. In keeping with the expressed Congressional intent, and in furtherance of the mission of DHS, information is being collected about covered individuals to enhance national security while facilitating legitimate travel and trade. In accordance with this purpose, US-VISIT collects, maintains, and shares information to determine whether the individual:

- Should be prohibited from entering the United States;
- Can receive, extend, change, or adjust immigration status;
- Has overstayed or otherwise violated the terms of his or her admission;
- Should be apprehended or detained for law enforcement action; or
- Needs special protection/attention (e.g., refugees).

Phase II of the International Live Test will provide an opportunity to test BAC of ICAO-compliant, international e-Passports against the selected U.S. document reader solution. BAC requires DHS readers to read the second line of the Machine Readable Zone (MRZ) in order to access the chip information.

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

The authorities for the US-VISIT Program include:

- The Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106-215, 114 Stat. 337;
- The Visa Waiver Permanent Program Act of 2000 (VWPPA), Public Law 106-396, 114 Stat. 1637;
- The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Public Law 107-565, 115 Stat. 271;
- The Enhanced Border Security and Visa Entry Reform Act of 2002 (The Border Security Act), Public Law 107-173, 116 Stat. 543;
- The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) Public Law 108-458, 118 Stat. 3775; and
- The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States.

The **DMIA** requires creation of an entry and exit system that integrates all available alien arrival and departure data maintained in electronic format in Department of Justice (DOJ)[1] or DOS databases. Under the DMIA, this integration of electronic arrival and departure information on an alien was required to be implemented at air and sea POEs no later than December 31, 2003; at the 50 most highly trafficked land border POEs by December 31, 2004; and at all POEs by December 31, 2005. The DMIA also requires DHS to use the entry and exit system to match the available arrival and departure data on aliens, and to prepare and submit reports to Congress on the numbers of aliens who have overstayed their periods of admission, as well as reports on the implementation of the system.

The **VWPPA** requires the creation of a system that contains a record of the arrival and departure of every alien admitted under the Visa Waiver Program (VWP) who arrives and departs by air or sea. The USA PATRIOT Act requires DHS and DOS jointly to develop and certify a technology standard that can be used to verify the identity of visa applicants and persons seeking to enter the United States pursuant to a visa, and to perform background checks on such aliens. The standard is required to include appropriate biometric identifier standards.

The **Border Security Act** requires that all VWP countries implement programs to issue ICAO-compliant, biometrically-enabled passports to their citizens. In addition, U.S. POEs must have the capability to compare and authenticate the biometric data in these passports. In interpreting this requirement, DHS required all applicants applying for admission under the VWP with passports issued on or after October 26, 2005, to have a passport that contains a digital photo. In addition, DHS has announced that any applicant applying for admission under VWP must be issued an e-Passport by October 26, 2006. These new e-Passports must comply with the international technical standards established by ICAO. DHS will acquire and install a document reader solution that reads e-Passports at U.S. POEs. DOS will issue ICAO-compliant e-Passports to U.S. citizens.

Additionally, the Act required DHS, in cooperation with other responsible agencies to install at all POEs by October 26, 2005, equipment and software that allow biometric comparison and authentication of all United States visas and all other machine-readable, tamper-resistant travel and entry documents issued to aliens. Public Law 108-299 extended the 118 Stat. 1100 implementation date from October 26, 2004 to October 26, 2005.

IRTPA consolidates the statutory authorizations for the US-VISIT program — a biometric entry and exit system — from the previous statutes. IRTPA combines the "integrated entry and exit system" described in DMIA with the "biometric" requirements described in the Border Security Act and the USA PATRIOT Act. IRTPA reiterates the clear Congressional intent for the creation of a biometric entry and exit system integrated with other applicable systems related to immigration policy, as the US-VISIT system has done.

The **9/11 Commission Report** calls for the implementation of a biometric screening system and specifically refers to the implementation of US-VISIT among the Commission's many recommendations for strengthening the ability of the United States to detect and deter terrorist attacks on the United States. The Report emphasizes the need to make US-VISIT fully operational as soon as possible and that the timetable in effect at the time of the Commission's consideration may have been too slow.

---

[1] Effective March 1, 2003, pursuant to the Homeland Security Act of 2002, Public Law 107-296, 116 Stat. 2135, the responsibility for maintenance of such files, along with other functions of the former Immigration and Naturalization Service, was transferred from DOJ to DHS.

The Privacy Act of 1974 specifically applies to U.S. citizens and Legal Permanent Residents (LPRs). DHS extended the Privacy Act protections to all individuals processed within the US-VISIT Program. Extension of the tenets of personal information protection means that US-VISIT will use best practices and efforts to ensure that any personal information collected will be appropriately stored, secured, and maintained.

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

No additional information will be collected from aliens. There will be no change to the current process for data collection and presentation. Phase II of the Live Test will not involve the collection of personal information beyond what is currently being collected from all travelers. During Phase II of the Live Test, the MRZ reads will be processed in the same manner in which they were previously processed. The primary difference is that all of the e-Passports involved in Phase II of the International Live Test have BAC incorporated into the passport. This means that the second line of the MRZ must be read in order to access the information stored on the chip. The chip contains the same data that is on the passport page of a legitimately issued passport. By displaying the information from the chip and comparing that information to the passport page, DHS will be able to confirm the authenticity and legitimacy of the document.

Section 2.0
Uses of the system and 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.

DHS uses the information collected and maintained by US-VISIT to carry out its national security, law enforcement, and immigration control functions. Through the enhancement and integration of its database systems, DHS is able to ensure the entry of legitimate travelers, identify, investigate, apprehend and/or remove individuals unlawfully entering or present in the United States beyond the lawful limitations of their visit, prevent the entry of inadmissible individuals, and detect fraud or abuse of U.S.-issued travel and entry documents. US-VISIT will also help DHS prevent covered individuals from obtaining immigration benefits to which they are not entitled. DHS may share information obtained through US-VISIT with other federal, state, local, and tribal enforcement partners to accomplish common law enforcement and national security goals.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as "datamining")?

US-VISIT does not currently have plans to implement data mining technology within the direct program environment. However, US-VISIT shares biographic and biometric information with DHS components, and other federal agencies that make use of data mining for the purposes of both investigative and intelligence gathering purposes.

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

In most cases, information is checked for accuracy when it is collected directly from the individual. For example, when a document's MRZ is scanned, the Customs and Border Protection (CBP) officer will check to ensure that the information is correct or the information can be corrected manually. Where information inaccuracies occur, a redress process is available as described below in Section 7.

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

US-VISIT uses a quality assurance process to identify any problem trends in properly matching individuals with relevant records, and vice versa, and to implement risk mitigation as needed, e.g., special checks targeted at specific data elements exhibiting a statistically significant tendency to cause matching errors. US-VISIT's redress process provides multiple points at which inaccurate data can be corrected, including on-the-spot corrections at POEs. In addition, all changes to individuals' immigration status that would result in enforcement actions undergo manual analysis and verification.

Section 3.0 Retention

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

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

US-VISIT employs multiple component systems, each of which has its own Privacy Act System of Records Notice (SORN). Each SORN specifies the retention policy that applies to that particular system. In some cases, however, a system has not been scheduled by the National Archives and Records Administration (NARA). The US-VISIT retention assessment that is currently underway in coordination with NARA and the DHS Records Management Office will result in a uniform retention policy for all US-

VISIT component systems that will be reflected in both the SORNs and the NARA retention schedules. Table 3-1 lists the retention policies for each US-VISIT component system as indicated by its SORN and by its NARA schedule.

Table 3-1. Existing Retention Policies of US-VISIT Component Systems

System	SORN Retention Policy	NARA Schedule
IDENT	Records for which the statute of limitations has expired for all criminal violations and that are older than 75 years will be purged	Awaiting NARA approval
ADIS	Records will be retained for 100 years	Awaiting NARA approval
TECS	Records are reviewed on a periodic basis to determine whether they should be purged	Records are retained for 40 years
AIDMS	Working with NARA to determine retention policy	To be determined

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

See Section 3.1.

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

Most of US-VISIT's component systems are legacy systems that were independently developed. As a result, their retention policies were also independently determined based on their legacy missions. Therefore, US-VISIT is working with NARA to develop a retention policy that can be uniformly applied to all component systems and that will appropriately address the needs of US-VISIT stakeholders. This process includes conducting interviews with both operational and records experts affiliated with each stakeholder to accurately capture retention requirements.

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 organizations is the information shared?

US-VISIT exchanges biographic and biometric information with the following internal entities:

Table 4-1. Information Sharing Matrix

Organization	System	Data Shared	Purpose
USCIS	CLAIMS 3	Biographic Information	Biographic Data Queries Benefits Adjudication
ICE	SEVIS	Biographic Information	Status Updates Benefits Adjudication
CBP	TECS	Biographic Information	Biographic Data Queries
	ADIS	Biographic Information	Entry and Exit Tracking

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

See Table 4-1 in Section 4.1.

4.3 How is the information transmitted or disclosed?

The information is electronically transmitted from each of the listed systems to IDENT. US-VISIT relies heavily on IDENT. However, IDENT contains both US-VISIT information and also information collected for other DHS programs. The US-VISIT program also relies on TECS to provide information to CBP officers.

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

DHS internal data sharing of US-VISIT information is required to comply with statutory requirements for national security and law enforcement. All of the information is kept secure, accurate, and is adequately controlled.

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 organizations is the information shared?

For the purposes of the US-VISIT program, DHS shares information with DOJ, the DOS, and the Department of Defense (DOD).

5.2 What information is shared and for what purpose?

For the purpose of the US-VISIT program DHS shares biometric and biographic information with the following external entities:

- DOS to support visa decision making;
- DOJ/ Federal Bureau of Investigation (FBI) for the purpose of national security or criminal investigations; and
- DOD in an effort to identify individuals who may pose national security threats.

Additionally, DHS may also share information with other agencies at the Federal, state, local, foreign, or tribal level who are lawfully engaged in collecting law enforcement information (whether civil or criminal) and national security intelligence information and/or criminal laws, related rules, regulations, or orders in accordance with the sharing agreement that exists between US-VISIT and the particular agency.

5.3 How is the information transmitted or disclosed?

Information is transmitted or disclosed to external organizations in one of three ways:

- Direct limited access to US-VISIT related systems where these organizations are co-located with DHS personnel with access to the systems;
- US-VISIT related systems have limited connections to other systems and US-VISIT information may be transmitted directly to those other systems; and
- Information collected through the US-VISIT process is securely transferred on portable media when there is no direct connection between systems.

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

DHS has entered into MOUs or other agreements with non-DHS organizations with which US-VISIT shares information. These agreements provide the conditions of sharing or disclosure, including governing the protection and use of the information. The appropriate/ relevant organizational entities that receive access currently have data sharing agreements in place with Federal, state, and local agencies for each system. These agreements are consistent with the US-VISIT privacy policy.

5.5 How is the shared information secured by the recipient?

External connections must be documented and approved with each party's signature in an interconnection security agreement (ISA) that outline controls in place to protect the confidentiality, integrity, and availability of information being shared or processed. Organizations with which US-VISIT shares information must agree to maintain reasonable physical, electronic, and procedural safeguards to appropriately protect the shared information. Furthermore, recipient organizations must notify US-VISIT as soon as reasonably practicable, but not later than within 24 hours, after they become aware of any breach of security of interconnected systems or unauthorized use or disclosure of personal information.

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

All information users must participate in a security and privacy training program. Consultants and contractors must also sign a non-disclosure agreement.

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

Because no new information is collected, Phase II of the Live Test will not result in any modifications to external sharing as reported in previous iterations of the US-VISIT PIAs. The existing sharing agreements provide for controls on what information is shared, how it is shared, and the use and retention of the information once the information is shared. US-VISIT sharing processes implement the Presidential Executive Order 13356 requirements to share terrorism-related information to the maximum extent consistent with law.

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

Notice is provided by means of publication of PIAs and SORNs published on the DHS website and in the Federal Register. Several rules and notices related to US-VISIT have also been published in the Federal Register. A complete list of the published PIAs, SORNs, rules, and notices is included in Appendix A.

In addition, US-VISIT has developed an aggressive outreach program that is making information on US-VISIT available to travelers as it is rolled out to new locations or to additional classes of travelers. These outreach efforts include press releases, press events, and advertising. Materials have also been developed for use by the airlines and cruise lines to explain the US-VISIT entry and exit process.

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

Individuals may decline to provide the requested information, but by doing so they may be denied entry into the United States or refused a visa. [2]

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

The admission into the United States of any covered traveler is contingent upon submission of the information required by US-VISIT, including biometric identifiers, as required. Failure to provide biometrics at the time of visa application or application for admission may result in visa refusal or denial of entry. A covered traveler who declines to provide required biometrics at the POE may withdraw his or her application for admission, or be subject to removal proceedings. The biometric requirement may be modified or waived at the discretion of the CBP secondary officer for those travelers with physical limitations or mental incapacity that prevent the collection of biometrics.

The US-VISIT Program has its own Privacy Officer to ensure that the privacy of all covered travelers is respected, and to respond to individual concerns raised about the collection of the required information. Extensive stakeholder outreach and information dissemination activities have taken place and will continue as the program is expanded. These activities are reviewed and adjusted on an ongoing basis to ensure maximum effectiveness. Further, the DHS Chief Privacy Officer, who serves as the administrative appellate

[2] An individual may apply for a discretionary waiver of inadmissibility under Section 212(d)(3) of the Immigration and Nationality Act, 8 U.S.C. 1182(d)(3).

review authority for all individual complaints and concerns about the Program, exercises comprehensive oversight of all phases of the Program to ensure that privacy concerns are respected throughout implementation.

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

Because no new information is collected, Phase II of the Live Test does not require modifications to notice, as reported in previous iterations of the US-VISIT PIA. Despite efforts to provide notice, it is often up to the travelers to take proactive steps to identify the US-VISIT requirements before they travel. Once they arrive at the border, notice has little real impact on the covered travelers: either they provide the information or they risk not being admitted to the United States.

Section 7.0
Individual 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 which allow individuals to gain access to their own information?

Individuals processed through US-VISIT are allowed to have their records reviewed for accuracy, relevancy, timeliness, or completeness at the POE. This is the first opportunity an individual is allowed access to his or her own information. Thereafter, individuals must request information directly through the US-VISIT Redress process.

7.2 What are the procedures for correcting erroneous information?

At the POE, an individual can allow on-the-spot data correction by permitting the CBP Officer to manually correct the individual's name, date of birth, flight information, and country specific document number and document type errors. For biometric types of data mismatches, the officer sends a data correction request to US-VISIT, or an individual may request that the US-VISIT Privacy Officer review his or her records.

The information needed to process the redress request is listed below:

Step 1. Submit a letter that states why you believe that your record is not accurate, relevant, timely, or complete, and specify the amendment or correction that you want. Individuals are encouraged to submit copies of any documentation they think would be helpful to process their request.

Step 2. The following information must also be provided in the individual's letter to verify identity and to properly process the request:

- Full Name as listed in your Passport and/or Visa
- Mailing Address
- Contact Telephone Number (Providing this is optional, but may facilitate follow-up if additional information is needed to process your request)
- Date and Place of Birth
- Date of Arrival and/or Departure from U.S.
- U.S. Port of Arrival and/or Departure
- Name of Airline or Sea Vessel (Providing this is optional, but may facilitate the processing of your request)
- Airline Flight Number or Cruise Line Ticket Number
- Passport Number and Country of Issuance
- U.S. Visa Number

An individual must sign his or her request and the signature must either be notarized or submitted under 28 U.S.C 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization.

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

The US-VISIT website, www.dhs.gov/us-visit, provides procedures and a Redress Request Form for correcting information. If individuals do not have access to the US-VISIT website, they may request a copy of the Redress Request Form and instructions directly from the Privacy Officer by calling (202) 298-5200. The US-VISIT Privacy Office has set a goal of processing redress requests within 20 business days based upon the number of requests. If an individual is not satisfied with the response received from US-VISIT, an individual can appeal his or her case to the DHS Chief Privacy Officer, who will conduct a review and provide final adjudication on the matter.

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

Not Applicable. Redress opportunities are provided through the US-VISIT website: www.dhs.gov/us-visit.

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

US-VISIT will continue its current redress process of providing individuals an opportunity to have access to their own information and have their information reviewed and corrected. US-VISIT frequently gets redress requests that are more appropriately addressed to other organizations within DHS. When practicable, these requests will be forwarded to the correct organization, or the requester will be notified of the appropriate agency for the request.

Section 8.0
Technical Access and Security

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

8.1 Which user group(s) will have access to the system?

The primary user groups are CBP officers, ICE agents, USCIS officers, and DOS consular officers who all have general access to US-VISIT information. Users from other external agencies have limited access that is described by the sharing agreement between that agency and US-VISIT. Other groups have limited access, including developers, workstation attendants, program managers, and information technology (IT) staff. These limits may be based on time, such as developers processing existing data as US-VISIT is developed and implemented, or the limit may be based on need, such as workstation attendants who will only have access to the information necessary to assist covered travelers during the exit transaction. Managers and IT staff have limited access based on their need to access the information.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Contractors have access to the system and to the information in the system. The extent of access will vary based on the need to fulfill the requirements of the contracts. Contractors currently having access to US-VISIT data include: the Smart Border Alliance, which includes Accenture and its sub-contractors, MITRE, and Nortel-PEC. Copies of the contracts have been submitted to the DHS Privacy Office.

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

Each of the specific systems – AIDMS, IDENT, TECS, and ADIS – assigns access to the information based on roles. Roles are created for each level of access required for individuals to perform their job functions. Examples of roles include basic user, system administrator, system auditor, and system manager.

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

US-VISIT has extensively documented and employed procedures for determining who may gain access to US-VISIT information and the extent of that access. The minimum requirements for access to US-VISIT information is documented in DHS and US-VISIT security documentation, and includes a DHS security clearance, security and privacy training, and need based on job responsibility.

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

Access roles are assigned by the system manager for each component and are reviewed regularly to ensure that users have the appropriate access. Individuals who no longer require access to US-VISIT information are immediately removed from the access list. Access is audited and the audit logs are reviewed on a regular basis.

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

ICAO-compliant e-Passports that employ BAC—including those issued by DOS—protect against both unauthorized access to the information contained within the chip and against inappropriate interception of information as it is transmitted from the chip to the reader. The second line of the MRZ must be read in order to unlock the chip. This process was specifically developed to eliminate the risk of surreptitious access. Once the chip is unlocked, the ensuing communication session is encrypted, thereby mitigating the risk of eavesdropping.

In general, the US-VISIT Program secures information and the systems on which that information resides by complying with the requirements of the DHS Information Technology Security Program Handbook. This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules, which are applied to component systems, communications between component systems, and at all interfaces between component systems and external systems.

US-VISIT follows the DHS Sensitive Systems Policy Directive 4300A as the source of information technology security policy. One aspect of the DHS comprehensive program to provide information security

involves the establishment of strict rules of behavior for each major application, including US-VISIT. The security policy also requires that all users be adequately trained regarding the security of their systems. Auditing logs are kept and reviewed on a regular basis.

The program also requires a periodic assessment of physical, technical, and administrative controls to enhance accountability and data integrity. All system users must participate in a security training program, and contractors and consultants must also sign a nondisclosure agreement. External connections must be documented and approved with each party's signature in an ISA, which outlines controls in place to protect the confidentiality, integrity, and availability of information being shared or processed. In addition, the comprehensive information technology security program already in effect for each of the component systems on which US-VISIT draws will be applied to the Program, adding an additional layer of security protection.

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

US-VISIT has developed a privacy training program that is given to all new US-VISIT employees and contractors. This training is also provided to individuals in other organizations who have access to the US-VISIT information. The privacy training provides a thorough introduction to the US-VISIT Privacy Policy, Privacy Principles, and Privacy Rules of Behavior. It describes both what is required of individuals handling personal information and the consequences of failing to comply with these requirements. Users also have annual refresher privacy training. In addition, throughout the year, users are provided with ongoing privacy awareness through newsletter articles, occasional memos, emails and other handouts highlighting specific privacy related issues. Specialized privacy training is provided to the exit workstation attendants. Specialized privacy training for other roles and for other special topics is currently in development.

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

The data is secured in accordance with DHS and national-level security requirements, including the FISMA requirements.

- AIDMS received an interim authority to operate in July 2005.
- IDENT was granted an authority to operate in May 2005.
- TECS was granted an authority to operate in February 2003.
- ADIS was granted an authority to operate in October 2003.

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

US-VISIT maintains a high degree of security to protect personal information in all its systems, as described in previous versions of the PIA. AIDMS is a new system in support of the RFID Proof of Concept (POC). Security risks have been assessed for AIDMS and mitigations have been put in place to protect US-VISIT data. Because the residual risks are deemed to be acceptable, the system is operating under an interim authority to operate, which is valid for six months. This authorization will remain in effect as long as the security posture of the system in maintained and the vulnerabilities reported under ongoing security monitoring do not result in unacceptable risk. Additional testing will be conducted to support a full authorization to operate when the system reaches its final deployment configuration.

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

US-VISIT is an integrated system of systems. Most of the component systems that US-VISIT employs—IDENT, ADIS, CLAIMS 3, SEVIS, CCD and TECS—were pre-existing systems developed by their pre-DHS legacy organizations. As part of its RFID POC activities, US-VISIT has developed an additional component system—AIDMS. In addition to its component systems, US-VISIT also incorporates a number of other technical elements, including workstations, exit devices, RFID tags and readers, and devices that capture biometrics. In general, US-VISIT has developed its technical systems and elements since initial inception by combining and customizing commercially available technologies.

Although most of the component systems existed previously to US-VISIT's inception, most have been modified to incorporate or facilitate the US-VISIT functionality.

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

US-VISIT uses a privacy risk management process based on information life cycle analysis and fair information principles.[3] Technical and programmatic design choices are informed by this approach, which analyzes proposed changes in terms of their life-cycle processes—collection, use and disclosure, processing,

[3] Fair information principles—notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress—form the basis of many statutes and codes, including the Privacy Act, and represent internationally accepted norms for the handling of personal information.

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.

9.3 What design choices were made to enhance privacy?

US-VISIT has made protecting the personal information of travelers one of its primary goals. Consequently, privacy considerations have been included in the design process from its inception.

9.4 Privacy Impact Analysis: Given the above choices regarding technology, what privacy impacts were considered and how were they resolved?

This PIA update reflects analysis of the design elements specific to Phase II of the International Live Test. The e-Passports will have BAC, which requires the second line of the MRZ to be read before the data from the chip is accessed. By displaying the information from the chip, DHS will be able to confirm the authenticity and legitimacy of the document. The addition of BAC is specifically to mitigate privacy risks associated with inappropriate interception of information.

Conclusion

This updated PIA focuses on changes to the US-VISIT Program resulting from Phase II of the International Live Test.

US-VISIT through its Privacy Officer and in collaboration with the DHS Chief Privacy Officer, will continue to track and assess privacy issues throughout the life of the US-VISIT Program and will address those issues by employing appropriate privacy risk mitigations as necessary.

Responsible Officials

Steve Yonkers, Privacy Officer
US-VISIT
Department of Homeland Security

Approval Signature

Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security