Privacy Impact Assessment Update
for the

US-VISIT Program

In Conjunction with the Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Ports of Entry

July 1, 2005

Contact Point
Steve Yonkers
US-VISIT Privacy Officer
245 Murray Lane, SW
Washington, DC 20538
(202) 298- 5200

Reviewing Official
Nuala O'Connor Kelly
Chief Privacy Officer
Department of Homeland Security
Arlington, VA 22202
(571) 227-3813

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

1. Introduction

United States Visitor and Immigrant Status Indicator Technology (US-VISIT) is the program established by the Department of Homeland Security (DHS) to implement an integrated entry and exit data system to record the entry into and exit out of the United States of covered individuals; verify identity; and confirm compliance with the terms of admission to the United States.

The primary goals of US-VISIT are to:

- 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.

In accordance with the guidance issued by the Office of Management and Budget (OMB) on September 26, 2003 for implementing the E-Government Act of 2002 and in an effort to make the program transparent and address any privacy concerns, DHS's Chief Privacy Officer directed that a Privacy Impact Assessment (PIA) be performed for the initial implementation of the program and that the PIA be updated as necessary to reflect future changes.

The US-VISIT PIA was first published on January 4, 2004, in conjunction with the initial deployment of US-VISIT. The PIA was updated on September 14, 2004,[1] to reflect inclusion of visa waiver program (VWP) travelers in US-VISIT, expansion of US-VISIT to the 50 busiest land border ports of entry (POE) and changes in the business processes used by DHS to share information with Federal law enforcement agencies. The PIA was updated on June 15, 2005 to include the Live Test to read ICAO-compliant biometrically enabled travel documents by October 26, 2005.

This revision of the PIA is prompted by the:

1. Implementation of technology (Exit devices) and processes for recording the exit of covered individuals from air and sea ports by December 31, 2005; and
2. The proof of concept for technology and processes for automatically recording the entry and exit of covered individuals at U.S. land border POEs using Radio Frequency Identification (RFID)-enabled I-94 Arrival/Departure Forms. The proof of concept of the capability will begin in August 2005 and, if successful, will be deployed to the 50 busiest land ports by December 31, 2007.

[1] 69 FR 57036, US-VISIT Privacy Impact Assessment, September 23, 2004.

2. Overview of US-VISIT Implementation

Congress has directed DHS to establish an integrated and automated entry and exit system to record the arrival and departure of aliens, verify their identities, and authenticate their travel documents through comparison of biometric identifiers. Implementation has proceeded in increments for a variety of policy and operational reasons. The incremental implementation has been tied primarily to the analysis of the best technology available to accomplish the goals of the program. The following timeline provides a high-level overview of the US-VISIT Increments, followed by a narrative description of those increments.

High-level Timeline for US-VISIT Increments

Increment	2004	2004	2004	2004	2005	2005	2005	2005	2006	2006
	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	1st Quarter	2nd Quarter
1A (Biometric Entry Air/Sea)	1/5/04 Competed implementation of air and sea entry capability		9/30/04 Added VWP travelers to US-VISIT							
1B (Biometric Exit Air/Sea)			8/3/04 Began pilot for exit capability at air and sea POEs				Estimated 8/1/05 Begin implementation of exit capability at additional air and sea POEs			
2A (Biometric comparison and Document authentication)				10/26/04 Extended e-enabling reader requirements to 10/26/05		6/15/05 Live Test for e-enabled travel document reader capability at one air POE	10/26/05 Begin implementation of e-enabled travel document reader capability at most POEs and begin US-VISIT coverage of all other aliens			
2B (Biometric Entry/ 50 land)				12/31/04 Completed implementation of biometric data collection at 50 busiest land border POEs						
2C (Facilitated land border)							7/31/05 Proof of concept for RFID capability at five land border POEs		3/31/06 Begin implementation of RFID capability at land border POEs	
3 (Entry/ remaining POEs)							Estimated 7/1/05 Begin implementation of biometric data collection at most remaining land POEs			

Increment 1A – Entry at Air and Sea Ports of Entry

Increment 1 was deployed on January 5, 2004, by modifying pre-existing databases to accommodate the collection and maintenance of additional data fields and to establish interfaces required to share data between DHS record systems concerning entry and exit at certain POEs of covered individuals. Covered individuals were defined in Increment 1 as nonimmigrant visa holders and VWP entrants traveling through air, sea, and land border POEs. Since implementation of Increment 1, DHS has been collecting biometrics – two digital index fingerscans and a digital photograph – for each covered individual. The details of Increment 1 are provided in the PIA published on January 4, 2004.

Increment 1B – Exit at Air and Sea Ports of Entry

Increment 1 also involved the testing of Exit devices to collect exit data. Three alternatives to collect exit data — a kiosk, a mobile device, and a combination of the two devices that uses a specially-configured mobile device to validate the receipt from the kiosk device[2]— were tested from October 2004 through May 2005. All were found to be useful in different environments and will be variously implemented based on the operational characteristics of each air and sea port. The changes to systems to accommodate Increment 1B included:

1. Development of the three alternative Exit devices to capture traveler biometric and biographic information and forward it to the Automatic Biometric Identification System (IDENT).
2. Modification to IDENT to accept and store the Exit Tracking Request and to search the US-VISIT biometric watch list and verify the traveler's identity against an arrival record.
3. Modification to IDENT to forward the Record of Departure to the Arrival and Departure Information System (ADIS).
4. Modification to ADIS to accept the Record of Departure from IDENT for use in confirmation on subsequent entry or exit by the traveler.

Increment 2A – Biometric Verification of VWP Passports and U.S.-Issued Travel Documents

Increment 2A provides the capability to biometrically compare and authenticate valid documents at all POEs. Under the requirements of the Enhanced Border Security and Visa Entry Reform Act (Border Security Act) of 2002, as amended:

- All VWP Countries must implement a program of issuing International Civil Aviation Organization (ICAO)-compliant passports that are tamper-resistant and incorporate biometric and documentation authentication identifiers by October 26, 2005[3]
- U.S. Ports of Entry must have the capability to read VWP ICAO-compliant biometrically enabled travel documents by October 26, 2005

[2] This is referred to as the Validator Alternative in US-VISIT documents.

[3] Congress extended the original implementation date of October 26, 2004 by one year.

As the next step in implementing these legislative requirements, an International Live Test will be conducted. Australia, New Zealand, and the U.S. are the participants in the International Live Test that will be conducted from June to September at the Los Angeles, CA Airport POE and at the Sydney, Australia Airport POE. The International Live Test will evaluate the operational impact of the new technology as well as the performance of the e-Passports and the reader solutions being tested. However, the International Live Test evaluation will be limited in scope due to the fact that only two of the Visa Waiver Program countries' passports will be tested. Other Visa Waiver Program countries' passports will have to be tested and evaluated as they begin the process of issuing e-Passports to their nationals.

In conjunction with implementation of Increment 2A, a Notice on Authority to Collect Biometric Data from Additional Travelers will be published on June 30, 2005. DHS intends to solicit comments on a proposal to further expand the population of "covered individuals" to include all aliens under US-VISIT, as required by statute. Increment 2A development and implementation will be analyzed in a future update to this PIA.

Increment 2B – 50 Busiest Land Ports of Entry

The deployment of Increment 2B was completed by December 31, 2004. It provided the US-VISIT capability to collect information on entries at the 50 busiest land border POEs. In addition, it reduced the time required for the completion of I-94, Arrival/Departure Forms. Prior to Increment 2B, I-94 forms were hand written by the travelers. Completion of the forms is now done by CBP officers who enter the data electronically and then print the form. The changes made to these systems for Increment 2B included modification of secondary workstations at land POEs to capture biographic and biometric information. The details of Increment 2B were provided in the PIA dated September 14, 2004.

Increment 2C – RFID at Land Ports of Entry

Increment 2C will provide the capability to automatically, passively, and remotely record the entry and exit of covered individuals using Radio Frequency Identification (RFID) tags. The RFID tag will be embedded in the I-94 Arrival/Departure Forms, and will use a unique ID number embedded in the tag to associate the I-94 holders with the tag. After the tag-enabled I-94 is issued to an individual, the ID number will be used as a pointer to the individual's biographic information located in the TECS database maintained by CBP. ADIS then receives and stores the crossing data from TECS. When the individual passes through the entry and exit lanes of a POE, the ID number will be read and used to retrieve the individual's immigration information for use in the entry and exit inspection processes by CBP officers.

US-VISIT conducted an operational alternatives assessment and determined that passive RFID technology best satisfied its requirements for this increment of the program. A proof of concept is being conducted for the Increment 2C capability to verify this assessment. The proof of concept will begin in August 2005.

A new DHS system of records, the Automated Identification Management System (AIDMS), has been created to link the unique and individually-assigned RFID tag number to existing biographic information received from TECS and the entry and exit event information for each covered individual crossing the land border. AIDMS is a new system and is separate from TECS, ADIS, IDENT and the other databases used in the US-VISIT process. AIDMS is undergoing the DHS certification and accreditation process, which includes having an approved detailed security plan and a comprehensive technical assessment of the risks of operating the system. A System of Records Notice (SORN) will be published at or about the time of publication of this PIA.

Changes to systems to accommodate Increment 2C include:

1. Development of the AIDMS to capture and store traveler border crossing events associated with RFID tag numbers and biographic information maintained in TECS.
2. Development of the antenna and reader capability to capture RFID tag numbers and to transmit the unique tag number and associated event information to AIDMS.
3. Modification of POE workstations to accept reads from RFID tag antennae and to process information from the RFID tag and associated information from AIDMS and from TECS.
4. Modification of TECS to enable direct interaction with AIDMS and pre-position information so that it can be rapidly accessed on the POE workstations by CBP officers.
5. Modification of ADIS to accept the RFID tag number from AIDMS via TECS.

Increment 3 – Remaining Land Ports of Entry

Increment 3 will extend the basic US-VISIT functionality introduced by Increment 2B to the remaining land border POEs. The changes to these systems for Increment 2B included modification of secondary workstations at land POEs to capture biographic and biometric information. In order to complete this rollout by December 31, 2005, implementation at some POEs will begin as early as July 2005. No additional changes to the architecture are anticipated for this Increment.

3. System Overview

What information is to be collected?

All aliens are subject to the principal data collection requirements and processes (including biometric collection, biographic collection, and watch list checks) of the US-VISIT Program. Because US-VISIT has been implemented in increments, currently covered individuals consist of nonimmigrant visa holders and VWP applicants for admission traveling through all air, sea, and land border POEs where US-VISIT has been implemented.[4] US-VISIT verifies the identity of these travelers and the authenticity of their U.S.-issued travel documents.

The information to be collected from covered individuals includes complete name, date of birth, gender, country of citizenship, 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 Increment 2C, a unique and individually-assigned RFID tag number for each traveler.

[4] DHS intends to fully implement its statutory authority to cover all aliens, but it intends to afford public notice and comment before determining the most appropriate way to implement the relevant statutes.

Why is the information being collected?

Numerous statutes require an entry/exit program to be put in place to verify the identity of covered individuals who enter or leave the United States. In keeping with 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 in order to determine whether the individual:

- Should be prohibited from entering the U.S.;
- 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).

What opportunities do individuals have to consent or decline to provide information?

The admission into the United States of any covered individual is contingent upon submission of the information required by US-VISIT, including biometric identifiers. A covered individual who declines to provide required biometrics is inadmissible.[5] An individual who declines to provide required biometrics 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 applicants 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 individuals 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 be continued 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 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.

What are the intended uses of the 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, and prevent the entry of inadmissible individuals. US-VISIT will also help DHS prevent covered individuals from obtaining immigration benefits to which they are not entitled. DHS may

[5] 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).

share information obtained through US-VISIT with other federal, state, local, tribal, and foreign law enforcement partners to accomplish common goals through data sharing agreements that address privacy and security concerns as well as operational requirements for sharing.

4. System Architecture

US-VISIT is a system of systems. US-VISIT accomplishes its goals primarily through the integration and modification of the capabilities of three pre-existing DHS systems and, with Increment 2C, through the creation of a new system, AIDMS. The pre-existing DHS systems are:

1. The Arrival and Departure Information System (ADIS)[6]
2. The Passenger Processing Component of the TECS[7]
3. The Automated Biometric Identification System (IDENT)[8]

US-VISIT interfaces with other DHS systems for relevant purposes, including status updates and benefit adjudication. In particular, US-VISIT exchanges biographic information with the Student and Exchange Visitor Information System (SEVIS) and the Computer Linked Application Information Management System (CLAIMS 3). Some of these systems, such as IDENT and the new AIDMS, are under the direct control of US-VISIT, while some systems are under the control of other organizational entities within DHS, including TECS and ADIS under CBP, SEVIS under Immigration and Customs Enforcement (ICE), and CLAIMS 3 under United States Citizenship and Immigration Services (USCIS).

US-VISIT interfaces with other, non-DHS systems for relevant purposes, including watch list updates and checks. In particular, US-VISIT receives biographic and biometric information from the Department of State's (DOS) Consular Affairs Consolidated Database (CCD) as part of the visa application process, and returns fingerscan information and watchlist changes.

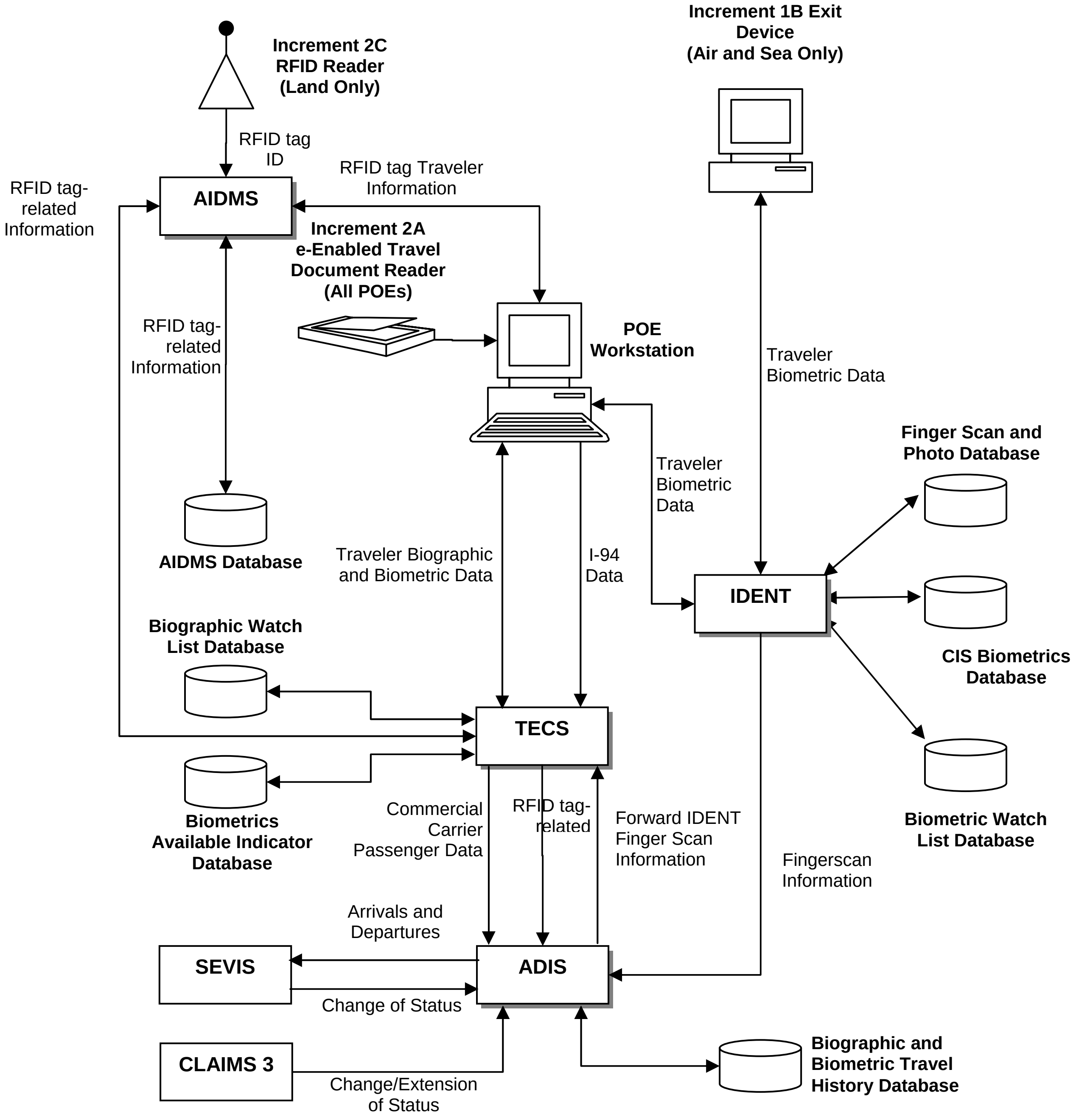
Figure 1 presents the data flows in the context of the high-level system architecture.

[6] System of Records Notice for Arrival and Departure Information System (ADIS), DHS/ICE-CBP-001, 68 FR 69412-69414 (December 12,2003).

[7] System of Records Notice for Treasury Enforcement Communications System (TECS), TREASURY/CS.244, 63 FR 60809 (December 17, 1998). As indicated in the US-VISIT Increment 1 Functional Requirements Document (FRD), the Passenger Processing Component of TECS consists of two systems, where "system" is used in the sense of the E-Government Act, 44 U.S.C. sec. 3502 (i.e., "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."). The two systems, and the process relevant to US-VISIT that they support, are (1) Interagency Border Inspection System (IBIS) (including the Nonimmigrant visa (NIV) database), supporting the lookout process; and (2) Advance Passenger Information System (APIS), supporting the entry/exit process by receiving airline passenger manifest information.

[8] System of Records Notice for Enforcement Operational Immigration Records (ENFORCE/IDENT), DHS/ICE-CBP-CIS-001, 68 FR 69414-69417 (December 12, 2003).

Figure 1: US-VISIT Architecture



5. Administrative Controls on Access to the Data

With whom will the information be shared?

Employees of DHS components, including CBP, ICE, and USCIS, and of DOS access the personal information collected and maintained by US-VISIT for immigration and border management purposes.

The information may also be shared 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 who are investigating, prosecuting, enforcing, or implementing civil and/or criminal laws, related rules, regulations, or orders. The Privacy Act SORNs for the systems on which US-VISIT draws provide notice as to the conditions of disclosure and routine uses for the information collected by US-VISIT. Any disclosure by DHS must be compatible with the purpose for which the information was collected. Additionally, any non-DHS agency granted direct access to this information must sign a data sharing agreement that will govern protection and usage of the information. US-VISIT currently has data sharing agreements in place with federal, state and local agencies for each system, which are consistent with the US-VISIT privacy policy and which require each agency to coordinate with DHS before taking any further action based on the shared data.

How will the information be secured?

The US-VISIT Program secures information and the systems on which that information resides by complying with the requirements of DHS information technology security policy, particularly the DHS Information Technology (IT) Security Program Handbook for Sensitive Systems (Attachment A to DHS Management Directive 4300.1). 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. In addition, ADIS (10/2003), TECS (2/2003), and IDENT (5/2004) have been individually certified and accredited as satisfying applicable DHS security requirements. The new system, AIDMS, has a certification plan under development that will adhere to the DHS security requirements for new systems.

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. 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 non-disclosure agreement. External connections must be documented and approved with both parties signature in an interconnection security agreement (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.

6. Information Life Cycle and Privacy Impacts

Overview

The following analysis is structured according to the information life cycle. For each life-cycle stage—collection, use and disclosure, processing, and retention and destruction—key issues are assessed, privacy risks are identified, and mitigation measures are discussed. Risks are related to fair information principles—notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress—that form the basis of many statutes and codes and which represent internationally accepted norms for the handling of personal information.[9] US-VISIT has its own set of privacy principles, which are based on the more well-known fair information principles. Table E-1 in Appendix E provides an overview of the kinds of privacy risks associated with US-VISIT and the general types of mitigation measures that address those risks.

General privacy risks resulting from the collection, use and disclosure, processing, and retention and destruction of personal information are mitigated by a privacy policy (available at http://www.dhs.gov/us-visit) supported and enforced by a comprehensive privacy program. This program includes a separate Privacy Officer for US-VISIT, mandatory privacy training for system operators, appropriate safeguards for data handling in accordance with existing procedures and guidelines, and ongoing consultation with stakeholders and representative organizations. Additionally, US-VISIT conducts periodic strategic reviews to ensure that the data collected are limited to that which is necessary for US-VISIT purposes.

US-VISIT has implemented a comprehensive redress process to facilitate the amendment or correction by individuals of data that are not accurate, relevant, timely, or complete. The full US-VISIT redress policy, including request form, is available at http://www.dhs.gov/us-visit. The US-VISIT Privacy Officer has set a goal of processing redress requests within 20 business days.

Increment 1B – Exit at Air and Sea Ports of Entry

Collection

The use of mobile Exit devices presents the low potential security risk that individuals might be persuaded by someone masquerading as an authorized official to allow their personal information and fingerprints to be captured by a counterfeit device. This risk is mitigated by workstation attendant (WSA) identification devices, appropriate training of airport staff, and awareness measures aimed at covered individuals (for example, signage that describes the precise circumstances under which covered individuals would be expected to undergo data collection). The physical size of the kiosks, along with the physical security at air and sea ports, which only allows ticketed passengers into the boarding area, makes it unlikely that someone could successfully collect personal data using a counterfeit device.

[9] Notice/awareness involves being informed of an entity's information handling practices and requires limitation of collection, use, disclosure, and retention to that which is consistent with stated purposes. Choice/consent requires that, to the extent possible, options be provided regarding the collection and handling of personal information. Access/participation involves the ability to view and/or contest the data held about oneself. Integrity/security requires that steps be taken to ensure that personal information is both accurate and protected. Enforcement/redress involves compliance mechanisms.

Use and Disclosure

US-VISIT conducted a privacy risk assessment of the privacy risks specific to the Exit pilot environment and the three alternative solutions that the Exit pilot was designed to evaluate. The risks associated with issuing receipts that include biographic and biometric data have been recognized and addressed by minimizing the amount of human readable information, minimizing biometric information, and encrypting machine readable biographic and biometric information.

The Exit devices generate a receipt for the covered individual to confirm that the exit process was successfully completed and, when a combination of kiosk and mobile device is used, to verify that the individual boarding at the gate is the same individual who completed the exit process at the kiosk. To enable this verification, the receipt printed by the kiosk includes biographic information read from the machine-readable zone (MRZ) of the individual's travel document and biometric data in the form of a low-resolution photograph and the individual's fingerscan. This information is stored in an encrypted bar code on the receipt. Receipts printed by mobile devices (when used alone) do not include this bar code. In all cases, receipts include a human-readable area with minimal personal information (name, date and time, departure port and terminal) along with a unique receipt number. The personal information printed in the human-readable area of the receipts is no greater than the information printed on other travel documents, including boarding passes. Therefore, the existence of the human readable areas represents a minimal security risk if a receipt is lost or stolen. The bar codes are encrypted in accordance with federal information processing standards (FIPS) 140-2 using site-specific keys that are changed daily. Moreover, the fingerscan templates on the receipt are one-way mathematical transformations of the actual fingerscans that, even if obtainable, would be extremely difficult to use for any purpose. These mitigations effectively address the security risks of the bar code.

Processing

Data flows between US-VISIT component systems and/or applications are encrypted using FIPS-compliant mechanisms. This includes the wireless transmissions from some of the Exit devices, in which the data itself is encrypted prior to transmission (rather than relying on encryption of the connection). As with the receipts, site-specific keys are used and changed daily. This greatly mitigates the security risks associated with wireless transmission. Although it is possible that the encrypted transmissions could be intercepted, the data would remain inaccessible and key variation would make unauthorized decryption extremely difficult. US-VISIT will use wired networks for the kiosks wherever practicable to lower the risk even further.

Retention and Destruction

Fingerscans and biographic information are also temporarily stored on the Exit devices. Under normal operating conditions, this information is securely transmitted to a server upon completion of each transaction, at which time the information is deleted so as to be unrecoverable. However, if an Exit device encounters communication problems, it will retain the information until it can be transmitted. To mitigate the security risk inherent in this situation, all personal information stored on Exit devices is encrypted in a FIPS-compliant manner using site-specific keys that change daily. Mobile Exit devices present additional security risk by virtue of their potential for being lost or stolen. This risk is mitigated by authentication of device users and appropriate physical and procedural controls, in addition to the measures described above.

The policies of the pre-existing individual component systems, as stated in the SORNs, govern the retention of personal information collected by US-VISIT. Because the component systems were created at different times for varied purposes, there are inconsistencies across the SORNs with respect to data retention periods. There is also some duplication in the types of data collected by each system. These inconsistencies and duplication result in some heightened degree of integrity/security, access, and/or redress risk as personal information could be deleted from one or more component systems while being retained in others. In order to most appropriately and effectively mitigate these risks, a comprehensive assessment of retention requirements has been initiated. When complete, this assessment will be used to establish a uniform retention policy for personal information collected by US-VISIT.

Increment 2C – RFID at Land Ports of Entry

Collection

Entry and exit data collected from the Form I-94 at land border POEs are transferred to a non-US-VISIT component of TECS. However, the unique ID number of the RFID tag embedded in the I-94 forms will be retained in the AIDMS. This system has been created to link the unique and individually-assigned RFID tag number to existing biographic information received from TECS and the entry and exit event information for each covered individual crossing the land border. The RFID tag number will not contain or be derived from any personal information. Otherwise, the continued expansion of US-VISIT capabilities to land border POEs provides for the same data collection as currently implemented at air, sea, and land POEs, with identical risks and mitigations, as discussed in previously published PIAs for US-VISIT.

Use and Disclosure

AIDMS is undergoing the DHS certification and accreditation process, which includes having an approved detailed security plan and a comprehensive technical assessment of the risks of operating the system. The certification and accreditation process will be completed before the proof of concept becomes operational. AIDMS is a new system and is separate from TECS, ADIS, IDENT and the other systems used by US-VISIT. A SORN will be published at or about the time of publication of this PIA.

While RFID tag numbers are not encrypted and could be subject to interception, the RFID tag contains no personal information and can only be used to obtain personal information when combined with other data within AIDMS. AIDMS is a secure database that can only be accessed by authorized personnel signed into authorized workstations that communicate with the AIDMS via a secure network.

Processing

The unencrypted information on the I-94 RFID tags is even more minimal than that on the exit process receipts. In this case, the only information contained and read is a unique identification number, which is linked to the individual's biographic information retrieved from TECS. AIDMS records the entry and exit data automatically captured at U.S. land border POEs for a particular RFID tag rather than for a specific individual. It is when this information on the RFID tag entries and exits along with the biographic information from TECS is sent to ADIS that the individual's complete travel history is created.

Over a covered individual's lifetime an individual may be issued more than one RFID-enabled I-94, each with a unique ID number. Only in rare circumstances where travelers request a supplemental I-94 under a different class of admission would more than one RFID-enabled I-94 be valid at any given time.

Two potential privacy risks have been identified and are addressed here. If the format or some other characteristic of the RFID tag number renders it recognizable as a US-VISIT RFID tag, this would allow an unauthorized reader to surreptitiously determine an individual's status (i.e., within US-VISIT covered population). However, it is contemplated that the unencrypted RFID tag number will not be structured in such a way that it can be used to identify the individual as a non-immigrant. There is also a low risk that the RFID tag could be used to conduct surreptitious locational surveillance of an individual; i.e., to use the presence of the tag to follow an individual as he or she moves about in the U.S. However, ensuring that RFID tag numbers do not exhibit properties that can be readily attributed to US-VISIT and using a limited radio frequency range effectively mitigates this risk. The design process is also taking into account methods of reducing eavesdropping and skimming possibilities.

Retention and Destruction

The Increment has the same retention and destruction issues as discussed with Increment 1B. In order to most appropriately and effectively mitigate the associated privacy risks, a comprehensive assessment of retention requirements has been initiated. When complete, this assessment will be used to establish a uniform retention policy for personal information collected by US-VISIT.

7. Design Choices (including whether a new system of records is being created)

US-VISIT was originally intended by Congress to address concerns with visa overstays, the number of illegal foreign nationals in the country, and overall border security issues. After September 11, 2001, terrorism-related concerns expanded the scope to include all aliens and added urgency to the development and deployment of this program. Many of the characteristics of US-VISIT were pre-determined because of legislation[10] enacted both before and after the events of September 11, 2001. These characteristics include, among others:

- Working with NIST to implement biometric standard for identifying and verifying foreign nationals;
- Use of biometric identifiers in travel and entry documents issued to foreign nationals, and the ability to read such documents at U.S. POEs;
- Integration of arrival/departure data on covered individuals, including data from commercial carrier passenger manifests; and
- Integration with other law enforcement and security systems.

[10] The legislation includes: the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law 104-208; The Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106-215; The Visa Waiver Permanent Program Act of 2000 (VWPPA), Public Law 106-396; The USA PATRIOT Act, Public Law 107-56; and The Enhanced Border Security and Visa Entry Reform Act ("Border Security Act"), Public Law 107-173.

Increment 1 – Exit at Air and Sea Ports of Entry

Three alternatives were evaluated for recording exit information at air and sea ports: kiosks, mobile devices, and a combination of the two devices that uses a specially-configured mobile device to validate the receipt from the kiosk device. In some cases, constraints on physical space rendered kiosks impractical. In other cases, boarding area layouts were not conducive to the use of mobile devices. The combination alternative was preferred for situations characterized by heightened security concerns. From a privacy perspective, the kiosk—particularly when using wired networks—introduces the fewest potential risks, followed by the mobile device (due to its portability), and finally, the combination alternative. Therefore, appropriate privacy risk mitigations are being implemented in order to successfully utilize all three alternatives. Examples of privacy-risk mitigation efforts include strong access controls to Exit devices, limited retention of data on the devices, privacy training for Exit workstation attendants, and encryption. These efforts added greater costs and complexity, but enabled operational needs to be satisfied in a privacy-protective manner.

Increment 2C – RFID at Land Ports of Entry

The requirement to facilitate land border traffic while capturing information about entries and exits has led to DHS developing a proof of concept for using RFID technology. In addition, US-VISIT has developed a new component system of records, the Automated Identification Management System (AIDMS), to enable the use of RFID tags for automatically recording entry and exit information at land border POEs.

Increment 2C will provide the capability to automatically, passively, and remotely record the entry and exit of RFID tags issued to covered individuals. For purposes of the proof of concept, the RFID tags will be embedded in the Forms I-94, Arrival/Departure documents and use a unique ID number to associate the I-94 holders with entry and exit data at U.S. land border POEs and link that information with biographic information for CBP officers to review. US-VISIT conducted an operational alternatives assessment and determined that passive RFID technology best satisfied the following defined criteria:

- Protect personal privacy by controlling the use of personal information outside of DHS systems and minimizing the surreptitious tracking of travelers outside the port of entry.
- The chosen technology and business process should require no direct action on the part of the traveler, driven by the need not to impede traveler movement across the border while facilitating legitimate travel and trade.
- Manage traveler border crossings from a distance, driven by the need to detect traveler departures while minimally impacting the unconstrained POE setting.
- No increase in wait times as a result of implementation.
- No degradation in level of service for exit lanes.
- No significant degradation in traffic patterns.
- Chosen technology should be currently commercially available and not require significant time or levels of research and development for deployment.

- Chosen technology should support ease of use, be compact in size, and not require any maintenance by the part of the traveler.

A solution incorporating passive RFID technology would not increase wait times, degrade the level of service at exit or degrade traffic patterns since the passive RFID tag could be read automatically with minimal need for traveler participation. Passive RFID, in this application, will also protect personal privacy by reading only a unique number from an embedded chip in a new Form I-94 that will be issued to travelers. The chip does not contain any information about the individual traveler – it contains only a unique code number linked to the specific Form I-94 for that specific traveler and the entry/exit data recorded in DHS systems. Passive RFID also minimizes privacy impacts and significantly reduces the chance of travelers being surreptitiously tracked in that it does not constantly transmit information or beacon a signal. Passive RFID does not require batteries or activation for use and does not cause undue burden or inconvenience on the traveler.

Other alternatives considered consisted of Global Positioning System (GPS) devices and various forms of RFID. GPS and active forms of RFID, which constantly transmit signals, were eliminated on privacy grounds due to their ability to facilitate locational surveillance. This resulted in the decision to use the passive RFID option, which transmits information only when activated by a reader as the preferred alternative. While passive RFID is not without privacy risks, it presents a lower level of risk that can be substantially mitigated. Moreover, capturing RFID tag identification numbers that do not contain any personal information presents fewer privacy (including security) risks than collecting biometrics in the relatively open primary processing environment of a land border POE.

A proof of concept is being conducted for the Increment 2C capability and will begin in August 2005. If the concept is proved to be successful, deployment to the 50 busiest land ports must be completed by December 31, 2007.

8. Summary and Conclusions

This updated PIA focuses on changes to US-VISIT resulting principally from Increment 1B implementation of technology (Exit devices) and processes for recording the exit of covered individuals from air and sea ports; and the Increment 2C proof of concept for technology and processes for automatically recording the entry and exit of covered individuals at U.S. land border Ports of Entry (POEs) using Radio Frequency Identification (RFID)-enabled I-94.

As a result of this analysis, it is concluded that:

- While most of the initial high-level design choices for US-VISIT were statutorily pre-determined, more recent design choices have been made so that privacy risks are either avoided or mitigated while meeting operational requirements;
- US-VISIT creates a pool of individuals whose personal information is at risk (covered individuals), which is effectively growing as a result of the expanded functionality, data sharing, and implementation of US-VISIT; but
- US-VISIT mitigates the specific privacy risks associated with its new functionality and increased data sharing through numerous mitigation efforts, including access controls,

education and training, encryption, minimizing collection and use of personal information; and

- 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 adjusting existing and implementing new privacy risk mitigations as necessary.

Appendix A: List of References

1. Statutory Authorities

1.1. Statutory Authorities for Protection of Information and of Information Systems

5 U.S.C. § 552, Freedom of Information Act (FOIA) of 1966, As Amended By Public Law No. 104-231, 110 Stat. 3048

5 U.S.C. § 552a, Privacy Act of 1974, As Amended

Public Law 100-503, Computer Matching and Privacy Act of 1988

Public Law 107-347, E-Government Act of 2002, Section 208, Privacy Provisions, and Title III, Information Security (Federal Information Systems Management Act (FISMA))

1.2. Statutory Authorities for US-VISIT

Public Law 104-208, Illegal Immigration Reform and Immigrant Responsibility Act of 1996

Public Law 106-215, The Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA)

Public Law 106-396, The Visa Waiver Permanent Program Act of 2000 (VWPPA)

Public Law 107-56, The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

Public Law 107-173, Enhanced Border Security and Visa Entry Reform Act of 2002 (“Border Security Act”)

1.3. Federal Register Notices and Rules

Department of Homeland Security; Implementation of the United States Visitor and Immigrant Status Indicator Technology Program; Biometric Requirements, 69 FR 468 (January 5, 2004).

Department of Homeland Security; Border and Transportation Security; Notice to Aliens Included in the United States Visitor and Immigrant Status Indicator Technology System, 69 FR 46556 (August 3, 2004).

Department of Homeland Security; United States Visitor and Immigrant Status Indicator Technology Program; Authority to Collect Biometric Data From Additional Travelers and Expansion to the 50 Most Highly Trafficked Land Border Ports of Entry, 69 FR 53318 (August 31, 2004).

Department of Homeland Security; United States Visitor and Immigrant Status Indicator Technology Program; Authority to Collect Biometric Data From Additional Travelers and Expansion to the 50 Most Highly Trafficked Land Border Ports of Entry, 69 FR 64964 (November 9, 2004).

2. US-VISIT and Component Systems Documentation

Arrival Departure Information System Data Elements Document (Sensitive but Unclassified) (Draft), November 10, 2003.

Consolidated Functional Requirements Document, US-VISIT, Increment 1, Information Technology Program Management Support, Draft, August 28, 2003.

Consolidated Interface Control Document, US-VISIT, Increment 1, Draft, August 28, 2003.

DHS/ICE Baseline Security Requirements for Automated Information Systems, July 18, 2003.

DHS Sensitive Systems Policy Directive 4300A, March 31, 2005.

DoS – Department of Homeland Security Visa Applicant – US-VISIT/IDENT Lookup Interface Control Document, Version 1.0, Department of State, October 31, 2003.

ePassport Reader Request for Proposal, March 16, 2005.

ICE Security Requirements, printed October 30, 2003.

Increment 2C Operational Alternatives Assessment (Draft), US-VISIT, January 31, 2005.

Increment 2C Preliminary Design Review, US VISIT, March 28, 2005.

Increment 2C Proof of Concept – Phase 1 Functional Requirements Document, US VISIT, March 11, 2005.

Increment 2C RFID Feasibility Study – Final Report (Draft), US-VISIT, January 12, 2005.

Interagency Border Inspection System (IBIS) Security Features User Guide, Official Use Only, October 2, 2003.

IT Security Program Handbook, Version 2.1, Sensitive Systems, Department of Homeland Security, 4300A, July 26, 2004.

Privacy Risk Assessment for US VISIT EXIT (Draft), Version 3.0, March 23, 2005.

Security Evaluation Report (SER) for the Automated Biometric Identification System (IDENT), SMI-0039-SID-214-RG-40391, March 10, 2003.

Security Evaluation Report (SER) for the Visa Waiver Permanent Program Act Support System Arrival Departure Information System (VWPPASS/ADIS), SMI-0039-SI-214-DTR-50446, October 8, 2003.

System of Records Notice for Arrival and Departure Information System (ADIS), DHS/ICE-CBP-001, 68 FR 69412 (December 12, 2003).

System of Records Notice for Enforcement Operational Immigration Records (ENFORCE/IDENT), DHS/ICE-CBP-CIS-001, 68 FR 69414 (December 12, 2003).

System of Records Notice for Nonimmigrant Information System (NIIS), JUSTICE/INS-036, 68 FR 5048 (January 31, 2003).

System of Records Notice for Treasury Enforcement Communications System (TECS), TREASURY/CS.244, 63 FR 69865 (December 17, 1998).

Treasury Enforcement Communications System (TECS) Functional Security Requirements Document, United States Customs Service, February 20, 2003.

The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program Increment 1 Concept of Operations: Process Flows and Operational Scenarios, Draft, July 15, 2003.

US-VISIT Information Brochure, undated.

US-VISIT Privacy Policy, November, 2003.

US-VISIT Program Overview (DHS briefing), undated.

US-VISIT Q&As: Background Information, Draft REV, October 17, 2003.

US-VISIT Redress Policy, April 15, 2004.

3. Related Guidance and Supporting Documentation

Federal Trade Commission, Privacy Online: A Report to Congress, June, 1998.

OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Memorandum M-03-22, September 26, 2003.

Risk Management Guide for Information Technology Systems, NIST Special Publication 800-30, January 2002.

Roles for the National Institute of Standards and Technology (NIST) in Accelerating the Development of Critical Biometric Consensus Standards for US Homeland Security and the Prevention of ID Theft, NIST, March 11, 2003.

Appendix B: List of Acronyms

AIDMS	Automated Identification Management System
ADIS	Arrival and Departure Information System
APIS	Advance Passenger Information System
BLSR	Baseline Security Requirements
CBP	Customs and Border Protection
CIS	Citizenship and Immigration Services
CLAIMS 3	Computer Linked Applications Information Management System
COA	Class of Admission
CCD	Consular Affairs Consolidated Database
CSRC	Computer Security Resource Center
CVT	Candidate Verification Tool
DHS	Department of Homeland Security
DMIA	Data Management Improvement Act
DoB	Date of Birth
DocKey	Document Key
DOS	Department of State
ED	Exit Device
ENFORCE	Enforcement Operational Immigration Records
FBI	Federal Bureau of Investigation
FIN	Fingerscan Identification Number
FIPS	Federal Information Processing Standard (140-2)
FOIA	Freedom of Information Act
FRD	Functional Requirements Document
GPS	Global Positioning System
I&A	Identification and Authentication
IAFIS	Integrated Automated Fingerscan Identification System
IBIS	Interagency Border Inspection System
ICD	Interface Control Document
ICE	Immigration and Customs Enforcement
ID	Identifier
IDENT	Automated Biometric Identification System
IFR	Interim Final Rule
IIRIRA	Illegal Immigration Reform and Immigrant Responsibility Act
IT	Information Technology

LEO ED	Law enforcement officer Exit Device
LPR	Lawful Permanent Resident
MOU	Memorandum of Understanding
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NIV	Nonimmigrant Visa
OMB	Office of Management and Budget
PA	Privacy Act
PIA	Privacy Impact Assessment
PICS	Password Issuance Control System
POD	Port of Departure
POE	Port of Entry
Pub. L.	Public Law
RFID	Radio Frequency Identification
SER	Security Evaluation Report
SEVIS	Student and Exchange Visitor Information System
SM/I	Systems Management and Integration
SOR	System of Records
SORN	System of Records Notice
SSN	Social Security Number
STARS	Service Technology Alliance Resources
TBD	To Be Determined
TECS	Treasury Enforcement Communications System
U.S.C.	United States Code
USCIS	United States Citizenship and Immigration Services
US-VISIT	United States Visitor Immigrant Status Indicator Technology
VWP	Visa Waiver Program
VWPPA	Visa Waiver Permanent Program Act
VWPPASS	Visa Waiver Permanent Program Act Support System
WAN	Wide Area Network
W/S	Workstation
WSA	Workstation Attendant

Appendix C: Data Flows Detailed

Pursuant to section 202 of the Enhanced Border Security and Visa Entry Reform Act of 2002, US-VISIT information will be integrated with other DHS databases and data systems, and US-VISIT information systems will be interfaced with data systems of other agencies US-VISIT exchanges data on a routine basis with the Student and Exchange Visitor Information System (SEVIS), the Computer Linked Applications Information Management System (CLAIMS 3), and the State Department's Consular Affairs Consolidated Database (CCD). However, US-VISIT information is logically separated from other data and users on the component systems, which are not dedicated US-VISIT systems.

Tables C-1 through C-4 detail the flows of personal information in US-VISIT. In general, internally generated administrative information (other than identifiers) that is associated with individuals is not included. However, information with special relevance for the treatment of individuals (e.g., Class of Admission) is included. Table C-1 defines sets of data elements that are handled as groups. To reduce complexity, the rest of the data flow tables refer, when appropriate, to these groups rather than to individual data elements. Table C-2 details the data flowing into and out of US-VISIT breaking it down by component system/application. Table C-3 indicates what personal information individual US-VISIT processes are using and which systems/applications are involved in those processes. Note that because the contexts of primary and secondary inspection are different for air/sea POEs and land border POEs, Table C-3 refers instead to core and extended inspection. Table C-4 charts the flows of personal information between US-VISIT systems/applications and directly between US-VISIT systems/applications and selected other systems. A comprehensive assessment of external interfaces is underway. These tables facilitate analysis of the personal data requirements of US-VISIT and identification of potentially unnecessary data collection or movement.

Table C-1: Data Aggregates

Aggregate Name	Data Elements
DocKey	• Complete name • Date of birth • Citizenship • Gender • Travel document o Type o Number o Date of issuance o Country of issuance • Fingerscan Identification Number (FIN) • Biographic and biometric watch list hit/match[11]
RFID Tag Traveler Profile	• RFID Tag ID number • US-VISIT ID number • First name Middle name • Last name • Date of birth • Travel document type • Travel document ID number • Travel document country of issuance
RFID Tag Read	• RFID Tag Location • Timestamp • RFID Tag status
RFID Tag Read Event	• RFID Tag ID number • Event ID number • Event type • Timestamp • Event location • Transaction ID • Equipment read ID numbers • Crossing direction
Biometric Data	• Fingerscans • Photograph

[11] This information is not retained in the event of a false positive.

Table C-1: Data Aggregates (continued)

Aggregate Name	Data Elements
Admission data	• Class of admission • Admit until date
Visa data	• First name • Last name • Visa o Class o Number o Entry (multiple or one time entry) o Issuance date o Expiration date • Passport type • Passport number • Gender • Date of birth • Nationality
Travel document data	Dependent on document type but may include • Complete name • Document o Number o Date of issuance • Country of issuance

Table C-1: Data Aggregates (continued)

Passenger manifest	• Complete name • Date of birth • Gender • Document o Country of issuance o Type o Number o Expiration date o Issue date • Nationality • Carrier code, number • Vessel seaport • Vessel name • PNR Number • Arrival country, airport • Departure country, airport • Arrival date & time/Departure date • U.S. destination address • Passenger status, status code
I-94 data	• Complete name • Date of birth • Citizenship • Gender • Passport number • Country of residence • Departure city • Visa city of issuance • Visa data of issuance • U.S. destination address

Table C-1: Data Aggregates (concluded)

Visa application	• State Department case ID • Applicant ID • Complete name • Gender • Date of birth • Country of birth • Nationality • Passport o Number o Type o Date of issuance o Country of issuance o City of issuance o Expiration date • Visa type • Visa class
Encounter data	• Encounter date and time • Encounter applicant ID • Travel document o Type o Country of issuance o Number • Date of birth • Eye color • Hair color • Height • Complete name • Nationality • Country of birth • Race • Gender • Weight • State Department ID
Audit log	• User ID • Date and time • System actions

Table C-2: US-VISIT Data In/Out by System/Application

System/Application	Data In	Data Out
TECS	Passenger manifest, admission data, photo (NIV), visa data (NIV), DocKey, RFID tag Traveler Profile, RFID tag Event Read, RFID tag Read	Visa data (NIV), passenger manifest, DocKey (including biographic watch list hit/match), photo (NIV), admission data, audit log, RFID tag Traveler Profile, RFID tag Event Read, RFID tag Read
IDENT	DocKey, photo, fingerscans, biographic data (watch list updates)	DocKey (including biometric watch list hit/match), fingerscans, audit log
ADIS	Passenger manifest, admission data, DocKey, complete name, DoB, gender, country of birth, nationality, U.S. destination address, visa class, visa number, passport number, country of issuance, SSN[12], alien number, I-94 number, POE, entry date, POD, departure date, admission data (current/requested), case status, SEVIS status change date, SEVIS ID (current/requested), RFID tag Traveler Profile, RFID tag Event Read, RFID tag Read	DocKey, complete name, DoB, gender, nationality, visa type, visa number, passport number, country of issuance, POE, entry date, POD, departure date, admission data, SEVIS ID, SEVIS status, status change date, audit log
Workstation	Travel document data, visa data, passenger manifest, DocKey (including biographic and biometric watch list hit/match), photo, fingerscans, admission data, I-94 data	Updated passenger manifest, DocKey, photo, fingerscans, admission data, I-94 data
Exit Device	Travel document data, biometric data	Travel document data, biometric data
Law Enforcement Officer Exit Device	Travel document data, biometric data	Travel document data, biometric data, verification of identity, watch list hits
Candidate Verification Tool (CVT)	Candidate & subject fingerscans, FINs, photos, verification history	Verification decision
Secondary Inspection Tool	Encounter data, FIN (previous encounter)	
AIDMS	RFID tag Traveler profile, RFID tag Read, RFID tag Read Event	RFID tag Traveler Profile, RFID tag Read, RFID tag Read Event

[12] Received from CLAIMS 3 for non-immigrants authorized to work.

Table C-3: US-VISIT Processes and Data Usage

Process	Subprocess	System/Application	Data Usage
Pre-Arrival	Visa application check	TECS, IDENT	Visa application, photo, fingerscans, FIN
	Manifest data check	TECS	Passenger manifest
	Biographical watch list check	TECS	Passenger manifest
	Visa data check	TECS	Passenger manifest, visa data (NIV)
	Passenger list analysis	TECS	Results of passenger manifest, biographical watch list, and visa data checks
Arrival (core)	Biometric verification	IDENT, Workstation	DocKey, fingerscans
	Biometric watch list check	IDENT, Workstation	DocKey, fingerscans
	Document – visa comparison	TECS, Workstation	Travel document data, visa data (NIV), photo (NIV)
	Manifest/Admission update	TECS, ADIS, Workstation	Passenger, manifest, admission data
	I-94 data entry	Workstation	I-94 data
Arrival (extended)	Queries	IDENT, Secondary Inspection Tool	Encounter data, complete name, gender, DoB, doc type, number, and country of issuance, FIN (previous encounter)
	Admission update	TECS, ADIS, Workstation	DocKey, admission data
	Biometric comparison and document authentication	TECS, Workstation	Visa data (NIV), photo (NIV)
Departure	Biometric verification	IDENT, Exit Device	DocKey, fingerscans
	Biometric watch list check	IDENT, Exit Device	DocKey, fingerscans

Table C-3: US-VISIT Processes and Data Usage (concluded)

Process	Subprocess	System/Application	Data Usage
Arrival/Departure reconciliation	Arrival/Departure correlation	ADIS	Passenger manifest, admission data
	Change of status	ADIS	Complete name, DoB, gender, nationality, visa type, visa number, passport number, country of issuance, POE, entry date, POD, departure date, admission data, SEVIS ID, SEVIS status, status change date
Watch list hit/match verification		IDENT, Candidate Verification Tool (CVT)	Candidate & subject fingerscans, FINs, photos, verification history
Audit log capture		TECS, IDENT, ADIS, AIDMS	User, date and time, system actions

Table C-4, Part 1: US-VISIT System/Application Interface Data Flows

From To	W/S	AIDMS	TECS	IDENT	ADIS	ED	LEO ED
Work-Station (W/S)		RFID tag Traveler Profile	DocKey, admission data, updated passenger manifest	DocKey, photo, fingerprints			
AIDMS			RFID tag Traveler Profile, RFID tag read event				
TECS	DocKey, admission data, visa data (NIV), photo (NIV), passenger manifest, status, RFID tag Traveler Profile				DocKey, passenger manifest, admission data, RFID tag Traveler Profile		
IDENT	DocKey				DocKey		Identity verification
ADIS			DocKey				
Exit Device (ED)				Travel document data, biometric data			
Law Enforcement Officer ED				Travel document data, biometric data			
CIS Biometric System				Biometric data and biographic text			
Secondary Inspection Tool (SIT)							
Candidate Verification Tool (CVT)				Verification decision			

From \ To	W/S	AIDMS	TECS	IDENT	ADIS	ED	LEO ED
SEVIS					Complete name, DoB, gender, nationality, visa type, visa number, passport number, country of issuance, POE, entry date, POD, departure date, admission data, SEVIS ID, SEVIS status, status change date		
CLAIMS 3					Complete name, DoB, gender, country of birth, nationality, U.S. destination address, passport number, country of issuance, SSN, alien number, I-94 number, entry date, admission data (current/requested), case status, SEVIS ID (current/requested)		
Dept. of Justice (DOJ) IAFIS				Fingerscans, biographic data			
Dept of State Consular Affairs Consoli- dated DB (CCD)			Visa data (NIV), photo (NIV), FIN	Visa data (refusal)			
Non US-VISIT (NUSV) TECS							

Table C-4, Part 2: US-VISIT System/Application Interface Data Flows

From To	SIT	CVT	SEVIS	CLAIMS 3	DOJ IAFIS	CCD	NUSV TECS
Work-Station (W/S)							I-94 data
AIDMS							
TECS							
IDENT	Encounter data, complete name, gender, DoB, doc type, number, and country of issuance, FIN (previous encounter)	Candidate & subject fingerscans, FINs, photos, verification history				Encounter data, watch list hits, FIN Change, Watchlist Change	
ADIS			Complete name, DoB, gender, nationality, visa type & number, passport number & country of issuance, POE, entry date, POD, departure date, admission data, SEVIS ID, SEVIS status, status change date				
Exit Device (ED)							
Law Enforcement Officer ED							
Secondary Inspection Tool (SIT)							
CIS Biometric System							
Candidate Verification							

From To	SIT	CVT	SEVIS	CLAIMS 3	DOJ IAFIS	CCD	NUSV TECS
Tool (CVT)							
SEVIS							
CLAIMS 3							
Dept. of Justice (DOJ) IAFIS							
Dept of State Consular Affairs Consolidated DB (CCD)							
Non US-VISIT (NUSV) TECS							

Appendix D: Security Safeguards for Privacy Protection Detailed

NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems (January 2002) identifies classes of safeguards for information system security. Technical safeguards are applied (1) within component systems, (2) to communications between component systems, and (3) at interfaces between component systems and external (i.e., non-US-VISIT) systems. Physical safeguards are generally provided by the facilities in which components systems are housed. Administrative and procedural safeguards are provided by rules of behavior, as discussed in Section 4 above.

The table below provides greater detail on the various physical and electronic measures employed to counter the various threats to the US-VISIT Program. Compliance of ADIS, the Passenger Processing Component of TECS, IDENT, AIDMS, and the POE workstations with ID-4300A, the BLSR, and the DHS Physical Security Handbook is assumed. As reflected in the table, the same safeguards can mitigate many different threats.

Table D-1: Privacy Threats and Mitigation Methods Detailed

Nature of Threat	Architectural Placement	Safeguard	Mechanism
Intentional physical threats from unauthorized external entities	ADIS	Physical protection	The ADIS database and application is maintained at a Department of Justice Data Center. Physical controls of that facility (e.g., guards, locks) apply and prevent entry by unauthorized entities.
Intentional physical threats from unauthorized external entities	Passenger Processing Component of TECS	Physical protection	The Passenger Processing Component of TECS is maintained on a mainframe by CBP. Physical controls of the TECS facility (e.g., guards, locks) apply and prevent entry by unauthorized entities.
Intentional physical threats from unauthorized external entities	IDENT	Physical protection	IDENT is maintained on an IBM cluster at a Department of Justice Data Center. Physical controls of the facility (e.g., guards, locks) apply and prevent entry by unauthorized entities.
Intentional physical threats from unauthorized external entities	POE Workstation, Exit Device	Physical protection	Physical controls may be specific to each POE. Assumed to be in compliance with BLSR and DHS Handbook 4300A.
Intentional physical threats from unauthorized external entities	AIDMS	Physical protection	Physical controls may be specific to each POE. The AIDMS central server will be in a US-VISIT data center. All locations are assumed to be in compliance with BLSR and DHS Handbook 4300A.
Intentional and unintentional electronic threats from authorized	US-VISIT-wide	Technical protection: Identification and authentication (I&A)	User identifier and password, managed by the Password Issuance Control System (PICS) and the LDAP System. Role-based access schema and auditing capabilities

Nature of Threat	Architectural Placement	Safeguard	Mechanism
(internal and external) entities			also in place. Issue to be addressed during system integration: Define procedures for correlation among different user identifiers (issued by PICS, LDAP and the legacy mechanisms in ADIS, the Passenger Processing Component of TECS, IDENT, and the POE workstations) to facilitate tracking and investigation of activities by individual users. [13]
Intentional and unintentional electronic threats from authorized (internal and external) entities	ADIS	Technical protection: I&A	User identifier and password in concert with role based access control and audit mechanisms to respond appropriately as required.
Intentional and unintentional electronic threats from authorized (internal and external) entities	IDENT	Technical protection: I&A	User identifier and password in concert with role based access control and audit mechanisms to respond appropriately as required.
Intentional and unintentional electronic threats from authorized (internal and external) entities	Passenger Processing Component of TECS	Technical protection: I&A	User identifier and password in concert with role based access control and audit mechanisms to respond appropriately as required.
Intentional and unintentional physical and electronic threat from unauthorized external entities	POE Workstation	Technical protection: I&A	User identifier and password in concert with role based access control and audit mechanisms to respond appropriately as required. US-VISIT, Increment 2 client software runs on Windows 2000 workstations connected to the DHS network, with associated policies and procedures.
Intentional and unintentional electronic threats from authorized (internal and external) entities	Exit Device	Technical protection: I&A	User identifier and password in concert with role based access control and audit mechanisms to respond appropriately as required.

[13] Access to information on the system depends on, and accountability for user actions is ensured by, I&A of users. As indicated in the table, US-VISIT components provide user ID / password mechanisms. US-VISIT is moving to a single client with a single sign-on capability that will be controlled using role-based access with user IDs and complex passwords. Until that solution is implemented there are both role-based access controls and multiple logons to access various component systems.

Nature of Threat	Architectural Placement	Safeguard	Mechanism
Intentional and unintentional electronic threats from authorized (internal and external) entities	AIDMS	Technical protection: I&A	Role based access control and audit mechanisms to respond appropriately as required.
Intentional and unintentional electronic threats from authorized (internal and external) entities	ADIS	Technical protection: Authorization and access control	Enforced by database management system, via ADIS application interface.
Intentional and unintentional electronic threat from authorized (internal and external) entities	IDENT	Technical protection: Authorization and access control	Enforced by database management system, via IDENT application interface.
Intentional and unintentional electronic threat from authorized (internal and external) entities	Passenger Processing Component of TECS	Technical protection: Authorization and access control	Enforced by database management system, via IBIS application interface.
Intentional and unintentional physical and electronic threat from unauthorized external entities	POE Workstation	Technical protection: Authorization and access control	Access to US-VISIT client applications is authorized, given that access to the workstation is granted. Access controls to US-VISIT data on ADIS, TECS, and IDENT are enforced by the other component systems.
Intentional and unintentional physical and electronic threat from unauthorized external entities	Exit Device	Technical protection: Authorization and access control	Access to US-VISIT client applications is authorized, given that access to the Exit devices is granted.
Intentional and unintentional physical and electronic threat from unauthorized external entities	AIDMS	Technical protection: Authorization and access control	Enforced by database management system
Intentional electronic and physical threat	ADIS, IDENT, Passenger Processing	Technical protection: Object reuse (identified under	Assumed to be in compliance with BLSR and DHS Handbook 4300A.

Nature of Threat	Architectural Placement	Safeguard	Mechanism
from internal entities	Component of TECS	system protections)	
Intentional electronic and physical threat from external entities	POE Workstation, Exit Device	Technical protection: Residual information protection	Issue to be addressed during system integration: How to ensure residual information protection on the POE Workstation for transient objects containing biometric or biographic information. See Encryption, below.[14]
Intentional electronic and physical threat from external entities	Exit Device	Technical protection: Residual information protection	Since individual devices are projected to handle approximately 500 transactions per day, in the case of a breach or exposure of data, the number of affected records will be minimal. Information to be retained only until a transaction is complete, then immediate transmission of captured data to the appropriate server. Use of FIPS 140-2 compliant encryption of stored data on each device.
Intentional electronic and physical threat from external entities	Registered Traveler receipt from Exit Device	Technical protection	Daily changing of encryption keys along with NIST-approved encryption to be utilized.
Intentional physical and electronic threats from external entities	POE Workstation	Technical protection: Encryption	Issue to be addressed during system integration: How will encryption be used to protect transiently stored biometric and biographic information? Will encryption address the residual information concern?
Intentional physical and electronic threats from external entities	Exit Device	Technical protection: Encryption	Daily changing of encryption keys along with NIST-approved encryption to be utilized.

[14] Some Port of Entry (POE) workstations and Exit Devices will store various personal information, if only transiently. Accountability for user actions is ensured by audit mechanisms. ADIS, the Passenger Processing Component of TECS, and IDENT provide auditing. The US-VISIT, Increment 1 Functional Requirements Document (FRD) states two audit requirements on the IDENT Client:
RTM 8.3-10 "The IDENT Client System shall capture the user ID of the user collecting store-and-forward biographic and biometric information."
RTM 8.3-20 "The IDENT Client System shall capture the user ID of the user submitting store-and-forward transactions to the EID."
Captured information is cached and retained in the workstation even after the encounter ends. It is not deleted until the authorized user logs out of the workstation. As a result of this approach, the risk arises that the captured user ID could be modified while stored on the workstation, thus impairing DHS's ability to ensure compliance with rules of behavior and impose penalties for noncompliance.

Nature of Threat	Architectural Placement	Safeguard	Mechanism
Intentional electronic threat from authorized and unauthorized entities	US-VISIT internal communication (between POE workstation, Passenger Processing Component of TECS, ADIS, IDENT, and AIDMS)	Technical protection: Protected communications and transaction privacy	Internal communications occur over the secured DHS WAN. The ICD states that exchange of data between all systems will be accomplished by a message queuing service, using IBM Websphere MQSeries. Websphere SSL and/or PKI capabilities are not currently used, but provide potential future capability for additional protection of the privacy of US-VISIT transactions.
Intentional electronic threat from authorized and unauthorized entities	US-VISIT communication (between POE workstation, and Passenger Processing Component of TECS, ADIS, IDENT, and AIDMS)	Technical protection: Encryption	At times, communications may occur over non-government-owned external networks. Two communication paths exist within the server for data transmission. Encryption of data, utilizing a FIPS 140-2-strength encryption schema for data passage provides data protection.
Intentional and unintentional electronic threat from authorized entities	US-VISIT-wide, Passenger Processing Component of TECS, ADIS, and IDENT	Technical protection: Audit	Any US-VISIT-specific audit trail requirements will be determined and documented as part of the US-VISIT, Increment 1 Release 2 requirements / design phase. Issue to be addressed during integration: Define procedures for use of the auditing capabilities of the Passenger Processing Component of TECS, ADIS, and IDENT, as well as Websphere, to facilitate tracking and investigation of transactions that span component systems?
Intentional and unintentional electronic threat from authorized entities	Exit Device	Technical protection: Audit	Identification and Authentication of authorized users by individual mobile device is in place.
Intentional and unintentional electronic threat from external and internal entities	POE Workstation	Technical protection: Audit	The US-VISIT, Increment 1 FRD requires that the IDENT Client System capture the user ID of the user collecting biometric and biographic information, and of the user submitting transactions to the Enforcement Integrated Database. Issues to be addressed during integration: • How will the captured data on the client be protected against modification or deletion?

Nature of Threat	Architectural Placement	Safeguard	Mechanism
			• If this captured data is considered to be a local audit trail (rather than a component of a store-and-forward transaction, deleted when the transaction is submitted), how and on what system will audit data from multiple clients be aggregated?
Intentional electronic threats from authorized and unauthorized external entities	External interfaces	Technical protection: Boundary protection (e.g., firewall, guard)	Not specified. For US-VISIT Increment 1, • Passenger Processing Component of TECS interfaces is internal to US-VISIT. • ADIS interfaces with SEVIS and CLAIMS 3. • IDENT interfaces with IAFIS via the IDENT/IAFIS Gateway Server interface, Production IDENT, and the Department of State Consular Affairs Consolidated Database
Intentional electronic threats from authorized and unauthorized external entities	Registered Traveler receipt generated from Exit Device	Technical protection	Human readable information is minimized for viewing. Sub-optimal stores of biometric information are employed. Non-human readable information is encrypted.
Unintentional electronic and physical threats from authorized external entities	External interfaces	Administrative protection: Routine use agreements	Memoranda of Understanding with appropriate parties have been completed. Agreements currently exist with the Department of State and the FBI.
Intentional electronic threats from authorized and unauthorized external entities	Exit Device	Administrative protection	Warnings need to be posted in appropriate traveler literature.
Intentional electronic threats from authorized and unauthorized external entities	Exit Device	Administrative/ Procedural protection	Provision of training and awareness for Workstation Attendants is required.

Appendix E: Privacy Threats and Mitigations

Table E-1: Overview of Privacy Threats and Mitigation Measures

Type of Threat	**Description of Threat**	**Type of Measures to Counter/Mitigate Threat**
Unintentional threats from insiders[15]	Unintentional threats include gaps in the privacy policy; mistakes in information system design, development, integration, configuration, and operation; and errors made by custodians (i.e., personnel of organizations with custody of the information). These threats can be physical (e.g., leaving documents in plain view) or electronic in nature. These threats can result in insiders being granted access to information for which they are not authorized or not consistent with their responsibilities.	These threats are addressed by a privacy policy consistent with Fair Information Practices, laws, regulations, and OMB guidance; (b) defining appropriate functional and interface requirements; developing, integrating, and configuring the system in accordance with those requirements and best security practices; and testing and validating the system against those requirements; and (c) providing clear operating instructions and training to users and system administrators.
Intentional threat from insiders	Threat actions can be characterized as improper use of authorized capabilities (e.g., browsing, removing information from trash) and circumvention of controls to take unauthorized actions (e.g., removing data from a workstation that has been not been shut off).	These threats are addressed by a combination of technical safeguards (e.g., access control, auditing, and anomaly detection) and administrative safeguards (e.g., procedures, training).
Intentional and unintentional threats from authorized external entities[16]	Intentional: Threat actions can be characterized as improper use of authorized capabilities (e.g., misuse of information provided by US-VISIT) and circumvention of controls to take unauthorized actions (e.g., unauthorized access to systems). Unintentional: Flaws in privacy policy definition; mistakes in information system design, development, integration, configuration, and operation; and errors made by custodians	These threats are addressed by technical safeguards (in particular, boundary controls such as firewalls) and administrative safeguards in the form of periodic privacy policy and practice compliance audits and routine use agreements and memoranda of understanding which require external entities (a) to conform with the rules of behavior and (b) to provide safeguards consistent with, or more stringent than, those of the system or program.
Intentional threats from external unauthorized entities	Threat actions can be characterized by mechanism: physical attack (e.g., theft of equipment), electronic attack (e.g., hacking or other unauthorized access, interception of communications), and personnel attack (e.g., social engineering).	These threats are addressed by physical safeguards, boundary controls at external interfaces, technical safeguards (e.g., identification and authentication, encrypted communications), and clear operating instructions and training for users and system administrators.

[15] Here, the term "insider" is intended to include individuals acting under the authority of the system owner or program manager. These include users, system administrators, maintenance personnel, and others authorized for physical access to system components.

[16] These include individuals and systems that are not under the authority of the system owner or program manager, but are authorized to receive information from, provide information to, or interface electronically with the system.