US-VISIT Program
Privacy Impact Assessment Update
International Live Test

June 15, 2005

US-VISIT

United States
Visitor and Immigrant Status Indicator Technology
Program Office

US-VISIT Program Privacy Impact Assessment

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.

This revision of the PIA is prompted by the Live Test to read ICAO-compliant biometrically enabled travel documents by October 26, 2005.

2. Overview of US-VISIT Implementation

This enhancement to the US-VISIT Program 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[2]
- U.S. Ports of Entry must have the capability to read VWP ICAO-compliant biometrically enabled travel documents by October 26, 2005

[1] 69 FR 57036, US-VISIT Privacy Impact Assessment, September 23, 2004.
[2] 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, 2005 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.

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.[3] 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, and digital fingerscans.

• 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).

[3] 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.

- **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.[4] 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 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. The pre-existing DHS systems are:

1. The Arrival and Departure Information System (ADIS)[5]
2. The Passenger Processing Component of the TECS[6]

[4] 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).

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

[6] 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

3. The Automated Biometric Identification System (IDENT)[7]

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, 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.

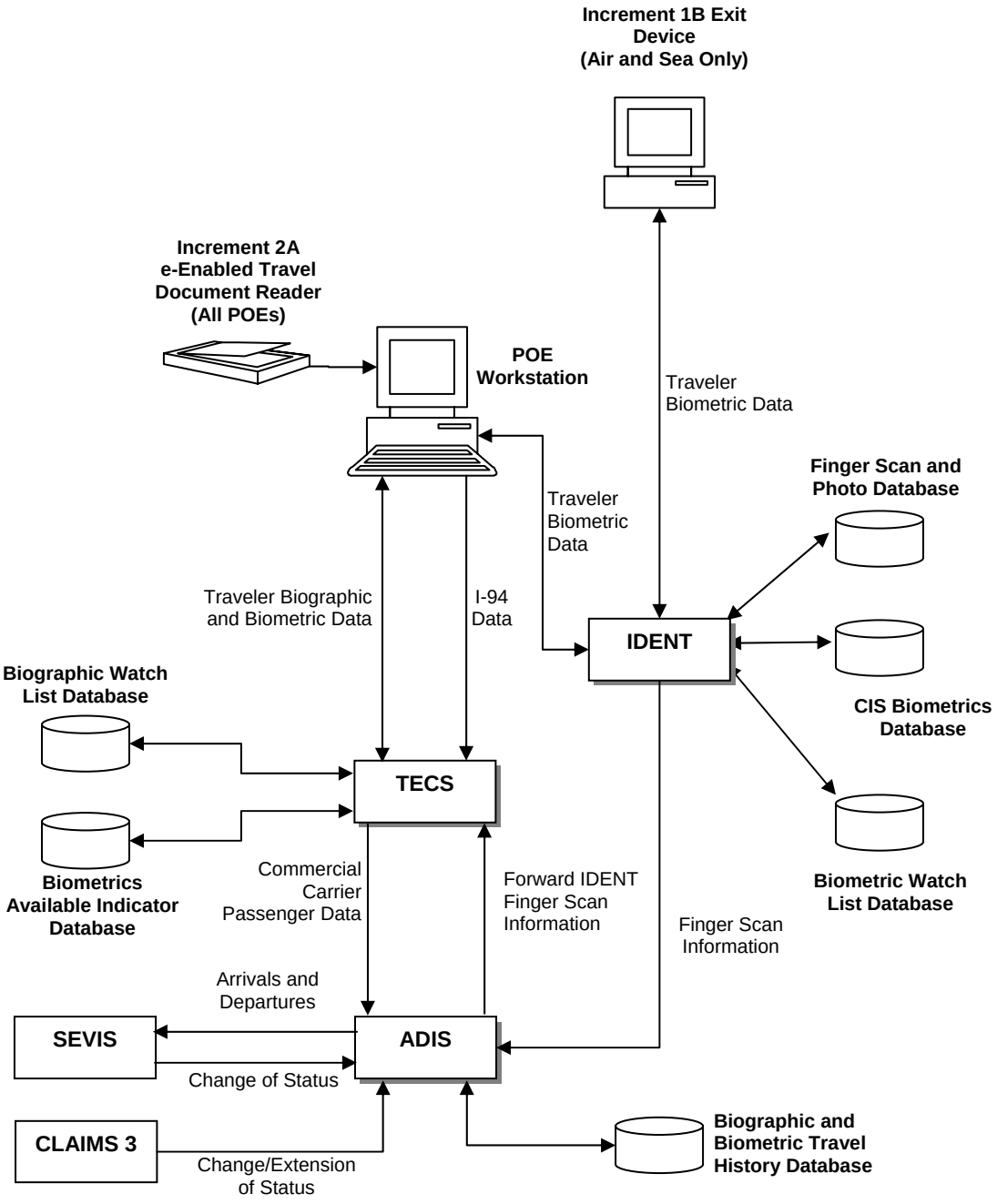
Figure 1 presents the data flows in the context of the high-level system architecture.

---

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.

[7] 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 System of Records Notices (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.

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.[8] 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 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 of the data to ensure that what is 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 www.dhs.gov/us-visit. The US-VISIT Privacy Officer has set a goal of processing redress requests within 20 business days.

Collection

The International Live Test (ILT) is to test biometrically enabled Passports (e-Passports) in a live environment, to assess e-Passport interoperability with the border management/inspection processes, and to biometrically verify US-issued travel documents. An additional goal is to test the ability of new and existing Reader Solutions for reading these documents, and the specific impact of the new technology on the operational border inspection processes. The test will involve the collection of data elements from the Machine Readable Zone (MRZ) on the biographic page of the e-Passport and will compare this information to the same data stored on the integrated contactless chip in the e-Passport. The chip will also display the digital image that is on the biographic page within the e-Passport; however, the photo will not be stored in the CBP processing system. DHS and DOS have requested NIST, the National Institute for Standards and Technology, to conduct security tests on the e-Passport reader solutions that are currently being evaluated for use for the Live Test. NIST testing began May 1, 2005, and the results are

[8] 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.

expected before full deployment of an e-Passport reader solution. The testing will be used to identify the potential for eavesdropping and jamming. Currently, lab and integration testing is ongoing to determine the maturity of the readers and interoperability with the current inspection system. However, DHS lacks the sample e-Passports from the various Visa Waiver Program countries to truly test a reader solution that is viable for full deployment.

Use and Disclosure

A passive device, such as the contactless chip in e-Passports, draws its transmitting power from the reader and the reader acts as the primary constraint on the read range. Once a reader powers the chip in an e-Passport, the transmission of an individual's personal information could be intercepted (i.e., subject to eavesdropping) therefore representing a potential security risk. Based on the results of NIST testing, the activity will include identification of optimal mitigation strategies (e.g., shielding of readers) and implementation of those strategies.

Processing

The Live Test will examine several e-Passport readers for their ability to interact with the existing passport processing infrastructure. The readers will be expected to read both the MRZ information and the contactless chip information. Once the information has been collected from the e-Passport, it will be displayed for the Customs and Border Protection (CBP) officer in the same manner as currently displayed. Since there is no new processing beyond the electronic read there do not appear to be any additional privacy concerns regarding processing of information beyond those described for the entire US-VISIT system.

The International Civil Aviation Organization (ICAO) standard defines additional fields for the integrated contactless chips that are not used in the inspection process in the United States. The software, however, is currently configured to retrieve data from only two places on the chip, including the MRZ information and the photo. At this point no other information will be retrieved.

Retention and Destruction

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[9] 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.

The Live Test is being conducted to determine the operational impacts of using new technology to read e-passports and to biometrically verify US-issued travel documents. During the test, legacy inspections equipment and processes will be utilized to capture baseline data. The scope of the test will encompass the entire Primary Inspection process. Data collection, such as duration of inspections and reader failure rates, will be captured automatically. Additionally, observers will monitor operations during the initial and final weeks of the 90-day test program. The results of the live test will be used to refine the final user requirements for implementation of the capabilities legislatively required.

Because this is a test of new equipment being used for the current process, the only privacy risks relate to issues of skimming or eavesdropping from the e-passports.

[9] 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.

8. Summary and Conclusions

This updated PIA focuses on changes to US-VISIT resulting from the Live POE Test of ICAO-compliant biometrically enabled travel documents (to be implemented by October 26, 2005).

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 2A Business Requirements, Version 3.0, US-VISIT, undated.

- Increment 2A Business Requirements, Version 1.0, US-VISIT, February 28, 2005.

- Increment 2A Concept of Operations, Version 1.3, US-VISIT, February 28, 2005.

- Increment 2A Live POE Test Plan, Draft Version 0.2, US-VISIT, March 17, 2005.

- Increment 2A Concept of Operations Live Port of Entry (POE) Test, Version 1.3, US-VISIT, February 10, 2005.

- Increment 2A – Project Charter, US-VISIT, February 9, 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.

- 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 Increment 2A Proposal, US-VISIT, April 11, 2004.

- 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

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
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
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
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

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[10]

Biometric Data	• Fingerscans • Photograph
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

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

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	Visa data (NIV), passenger manifest, DocKey (including biographic watch list hit/match), photo (NIV), admission data, audit log
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[11], 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)	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
Candidate Verification Tool (CVT)	Candidate & subject fingerscans, FINs, photos, verification history	Verification decision
Secondary Inspection Tool	Encounter data, FIN (previous encounter)	

[11] 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	User, date and time, system actions

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

From / To	W/S	TECS	IDENT	ADIS
Work-Station (W/S)		DocKey, admission data, updated passenger manifest	DocKey, photo, finger-prints	
TECS	DocKey, admission data, visa data (NIV), photo (NIV), passenger manifest, status			DocKey, passenger manifest, admission data
IDENT	DocKey			DocKey
ADIS		DocKey		
CIS Biometric System			Biometric data and biographic text	
Secondary Inspection Tool (SIT)				
Candidate Verification Tool (CVT)			Verification decision	
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
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				
Secondary Inspection Tool (SIT)							
CIS Biometric System							
Candidate Verification Tool (CVT)							
SEVIS							
CLAIMS 3							
Dept. of Justice (DOJ) IAFIS							
Dept of State Consular Affairs Consoli-dated 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	Physical protection	Physical controls may be specific to each POE. Assumed to be in compliance with BLSR and DHS Handbook 4300A.
Intentional and unintentional electronic threats from authorized (internal and external) entities	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 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

[12] 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
			workstations) to facilitate tracking and investigation of activities by individual users. [12]
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	ADIS	Technical protection: Authorization and access control	Enforced by database management system, via ADIS application interface.

Nature of Threat	Architectural Placement	Safeguard	Mechanism
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 electronic and physical threat from internal entities	ADIS, IDENT, Passenger Processing Component of TECS	Technical protection: Object reuse (identified under system protections)	Assumed to be in compliance with BLSR and DHS Handbook 4300A.
Intentional electronic and physical threat from external entities	POE Workstation	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,

[13] 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.”

Nature of Threat	Architectural Placement	Safeguard	Mechanism
			below.[13]
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 electronic threat from authorized and unauthorized entities	US-VISIT internal communication (between POE workstation, Passenger Processing Component of TECS, ADIS, and IDENT)	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, and IDENT)	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	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.

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
	TECS, ADIS, and IDENT		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 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
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.

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[14]	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.

[14] 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.

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[15]	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] 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.