US-VISIT Program, Increment 1
Privacy Impact Assessment

December 18, 2003

Contact Point

Steve Yonkers
US-VISIT Privacy Officer
Department of Homeland Security
(202) 298-5200

Reviewing Official

Nuala O'Connor Kelly
Chief Privacy Officer
Department of Homeland Security
(202) 772-9848

US-VISIT Program, Increment 1
Privacy Impact Assessment

1. Introduction

Congress has directed the Executive Branch to establish an integrated entry and exit data system to accomplish the following goals[1]:

1. Record the entry into and exit out of the United States of covered individuals;
2. Verify the identity of covered individuals; and
3. Confirm compliance by visitors with the terms of their admission into the United States.

The Department of Homeland Security (DHS) proposes to comply with this congressional mandate by establishing the United States Visitor and Immigration Status Indicator Technology (US-VISIT) program. The first phase of US-VISIT, referred to as Increment 1, will capture entry and exit information about non-immigrant visitors whose records are not subject to the Privacy Act. Rather than establishing a new information system, DHS will integrate and enhance the capabilities of existing systems to capture this data. In an effort to make the program transparent, as well as to address any privacy concerns that may arise as a result of the program, DHS's Chief Privacy Officer has directed that this PIA be performed in accordance with the guidance issued by OMB on September 26, 2003. As US-VISIT is further developed and deployed, this PIA will be updated to reflect future increments.

2. System Overview

• What information is to be collected

Individuals subject to the data collection requirements and processes of Increment 1 of the US-VISIT program ("covered individuals") are nonimmigrant visa holders traveling through air and sea ports. The DHS regulations and related Federal Register notice for US-VISIT Increment 1 will fully detail coverage of the program.

The information to be collected from these 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. address, arrival and departure information, and for the first time, a photograph, and fingerprints. US-VISIT will capture and store this information from existing systems that already record it or are being modified to allow for its collection.

[1] Congress enacted several statutory provisions concerning an entry exit program, including provisions in: 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 U.S.A. PATRIOT Act, Public Law 107-56; and The Enhanced Border Security and Visa Entry Reform Act ("Border Security Act"), Public Law 107-173.

- **Why the information is being collected**

In numerous statutes, Congress has indicated that an entry exit program must be put in place to verify the identity of covered individuals who enter or leave the United States. In keeping with this expression of congressional intent and in furtherance of the mission of the Department of Homeland Security, the purposes of US-VISIT are to identify individuals who may pose a threat to the security of the United States, who may have violated the terms of their admission to the United States, or who may be wanted for the commission of a crime in the U.S. or elsewhere, while at the same time facilitating legitimate travel.

- **What opportunities individuals will have to decline to provide information or to consent to particular uses of the information and how individuals grant consent**

The admission into the United States of an individual subject to US-VISIT requirements will be contingent upon submission of the information required by US-VISIT, including biometric identifiers. A covered individual who declines to provide biometrics is inadmissible to the United States, unless a discretionary waiver is granted under section 212(d)(3) of the Immigration and Nationality Act. Such an individual may withdraw his or her application for admission, or be subject to removal proceedings. US-VISIT has its own privacy officer, however, to ensure that the privacy of all visitors is respected and to respond to individual concerns which may be raised about the collection of the required information. Further, the DHS Chief Privacy Officer will exercise comprehensive oversight of all phases of the program to ensure that privacy concerns are respected throughout implementation. The DHS Chief Privacy Officer will also serve as the review authority for all individual complaints and concerns about the program.

3. Increment 1 System Architecture

US-VISIT Increment 1 will accomplish its goals primarily through the integration and modification of the capabilities of three existing systems:

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

US-VISIT Increment 1 will also involve modification and extension of client software on Port of Entry (POE) workstations and the development of departure kiosks.

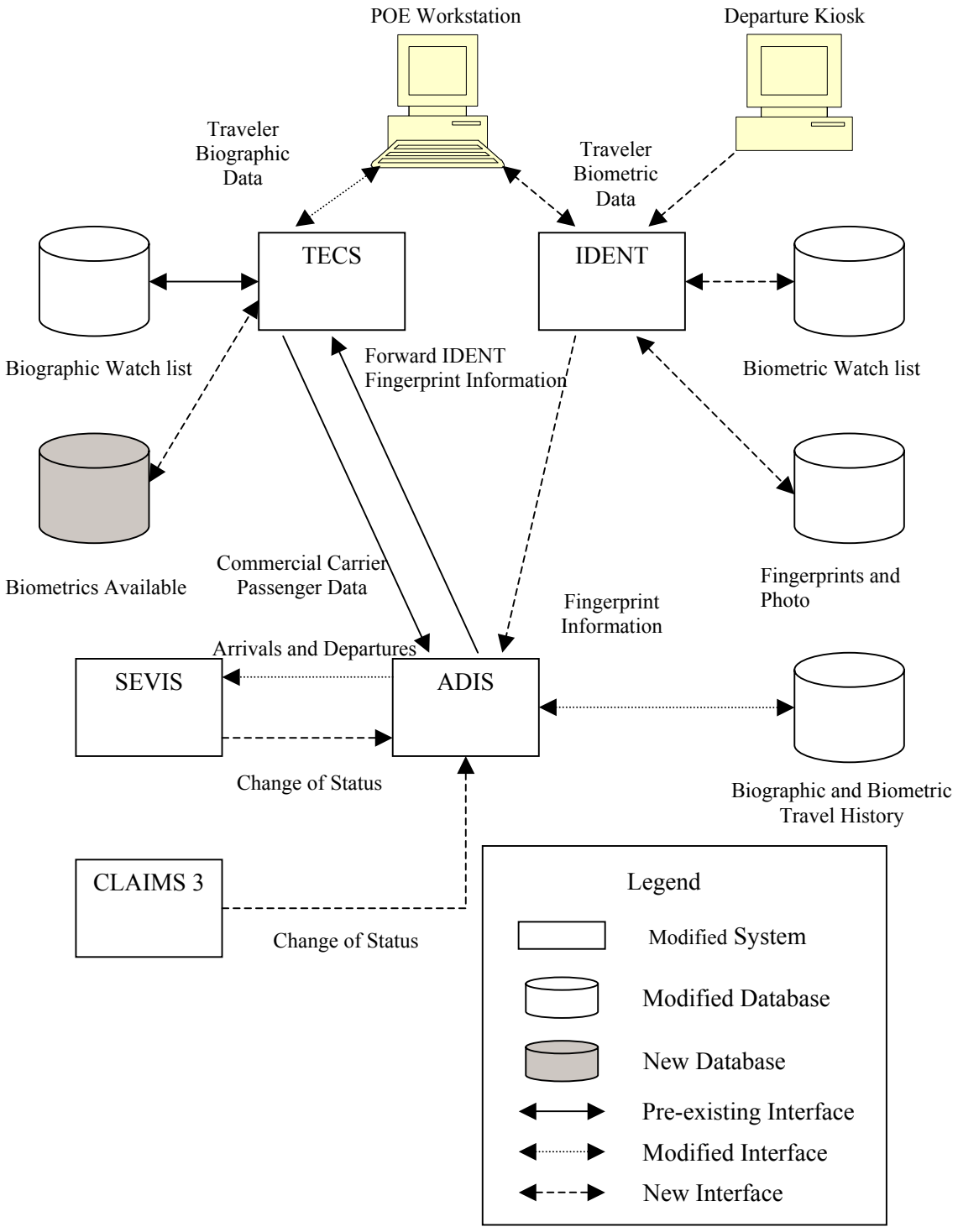
The changes to these systems include:

[2] 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, title 44, Chapter 35, section 3502 of US Code; 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 Increment 1 that they support, are (1) Interagency Border Inspection System (IBIS), supporting the lookout process and providing interfaces with the Interpol and National Crime Information Center (NCIC) databases; and (2) Advance Passenger Information System (APIS), supporting the entry process by receiving airline passenger manifest information.

1. Modifications of TECS to give immigration inspectors the ability to display non-immigrant-visa (NIV) data.
2. Modifications to the ADIS database to accommodate additional data fields, to interface with other systems, and to generate various types of reports based on the stored data.
3. Modifications to the IDENT database to capture biometrics at the primary port of entry (POE) and to facilitate identity verification.
4. Establishment of interfaces to facilitate the transfer of biometric information from IDENT to ADIS and from ADIS to TECS.
5. Establishment of other interfaces to facilitate transfer of changes in the status of individuals from two other data bases—the Student and Exchange Visitor Information System (SEVIS) and the Computer Linked Application Information Management System (CLAIMS 3) to ADIS.

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

Source: US-VISIT Increment 1 Functional Requirements Document



- **Intended use of the information**

DHS intends to use the information collected and maintained by US-VISIT Increment 1 to carry out its national security, law enforcement, immigration control, and other functions. Through the enhancement and integration of existing database systems, DHS will be able to ensure the entry of legitimate visitors, identify, investigate, apprehend and/or remove aliens unlawfully entering or present in the United States beyond the lawful limitations of their visit, and prevent the entry of inadmissible aliens. US-VISIT thus will enable DHS to protect U.S. borders and national security by maintaining improved immigration control. US-VISIT will also help prevent aliens from obtaining benefits to which they are not entitled.

4. Maintenance and Administrative Controls on Access to the Data

- **With whom the information will be shared**

The personal information collected and maintained by US-VISIT Increment 1 will be accessed principally by employees of DHS components—Customs and Border Protection, Immigration and Customs Enforcement, Citizenship and Immigration Services, and the Transportation Security Administration–and by consular officers of the Department of State. Additionally, the information may be shared with other law enforcement agencies at the federal, state, local, foreign, or tribal level, who, in accordance with their responsibilities, are lawfully engaged in collecting law enforcement intelligence information (whether civil or criminal) and/or investigating, prosecuting, enforcing, or implementing civil and/or criminal laws, related rules, regulations, or orders. The system of records notices for the existing systems on which US-VISIT draws provide notice as to the conditions of disclosure and routine uses for the information collected by US-VISIT, provided that any disclosure is compatible with the purpose for which the information was collected.

US-VISIT transactions will have a unique identifier to differentiate them from other IDENT transactions. This will allow for improved oversight and audit capabilities to ensure that the data are being handled consistent with all applicable federal laws and regulations regarding privacy and data integrity.

- **How the information will be secured**

The US-VISIT program will secure information and the systems on which that information resides, by complying with the requirements of the DHS IT Security Program Handbook. This handbook establishes a comprehensive program, consistent with federal law and policy, to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, and application rules, which will be applied to component systems, communications between component systems, and at interfaces between component systems and external systems.

One aspect of the DHS comprehensive program to provide information security involves the establishment of rules of behavior for each major application, including US-VISIT. These rules of behavior require users to be adequately trained regarding the security of their systems. These rules also require a periodic assessment of technical, administrative and managerial controls to enhance data integrity and accountability. System users must sign statements acknowledging that they have been trained and understand the security aspects of their systems. In addition, the

rules of behavior 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.

The table below provides detail on the various measures employed to address potential security threats to US-VISIT Increment 1.

Security 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 entrée 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 entrée by unauthorized entities.
Intentional physical threats from external entities	IDENT	Physical protection	IDENT is maintained on an IBM cluster. Physical controls of the facility (e.g., guards, locks) apply and prevent entrée by unauthorized entities.
Intentional physical threats from external entities	POE Workstation	Physical protection	Physical controls will be specific to each POE.
Intentional and unintentional electronic threats from authorized (internal and external) entities	System-wide	Technical protection: Identification and authentication (I&A)	User identifier and password, managed by the Password Issuance Control System (PICS).

5. Information Life Cycle and Privacy Impacts

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 identified, and mitigation measures 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.

• Collection

US-VISIT Increment 1 collects only the personal information necessary for its purposes. While Increment 1 does not constitute a new system of records, it does expand the types of data held in its component systems to include biometric identifiers. By definition this creates a general privacy risk. This risk is mitigated, however, by establishment of a privacy policy supported and enforced by a comprehensive privacy program. This program includes a separate Privacy Officer for US-VISIT, mandatory privacy training for system operators, and appropriate safeguards for data handling.

- **Use and Disclosure**

The IDENT and TECS systems collect data that are used for purposes other than US-VISIT. As a result, data collected for US-VISIT through these systems may become available for another functionality embodied in these component systems. This presents a potential notice risk: will the data be used for a purpose consistent with US-VISIT? This risk is mitigated in several ways. First, US-VISIT isolates US-VISIT data from non US-VISIT data on component systems, and users will be subject to specific privacy and security training for this data. Second, the IDENT and TECS systems already have their own published SORNS, which explain the uses to which the data they collect will be put, for US-VISIT as well as non-US-VISIT purposes. This, too, mitigates the notice risk. Third, Memoranda of Understanding and of Agreement are being negotiated with third parties (including other agencies) that will address protection and use of US-VISIT data, again to mitigate this notice risk.

- **Processing**

Data exchange, which will take place over an encrypted network between US-VISIT Increment 1 component systems and/or applications is limited, and confined only to those that are functionally necessary. Although much of the personal information going into ADIS from SEVIS and CLAIMS 3 is duplicative of data entering ADIS from TECS, this duplication is to ensure that changes in status received from SEVIS or CLAIMS 3 are associated with the correct individual, even in cases of data element mismatches (i.e., differing values for the same data element received from different sources). This mitigates the data integrity risk. A failure to match generates an exception report that prompts action to resolve the issue. This also mitigates integrity risk by guarding against incorrect enforcement actions resulting from lost immigration status changes. (The data flows from SEVIS and CLAIMS 3 principally support changes in status.)

On the other hand, if a match is made, but there are some data element mismatches, no report is generated identifying the relevant records and data elements (one or more of which must have inaccurate or improper values) and no corrective action is taken. This is due to the resources that would be required to investigate all such events. This integrity risk again creates a possibility of incorrect enforcement actions if the match was made in error as a result of the data element mismatches. However, this aspect of the integrity risk is mitigated by subjecting all status changes that would result in enforcement actions to manual analysis and verification. A quality assurance process will also be used to identify any problem trends in the matching process.

- **Retention and Destruction**

The policies of individual component systems, as stated in their SORNs, govern the retention of personal information collected by US-VISIT. Because the component systems were created at different times for different purposes, there are inconsistencies across the SORNs with respect to data retention policies. There is also some duplication in the types of data collected by each system. These inconsistencies and duplication result in some heightened degree of risk with respect to integrity/security of the data, and to access and redress principles, because personal information could persist on one or more component systems beyond its period of use or disappear from one or more component systems while still in use. These risks are mitigated, however, by having a Privacy Officer for US-VISIT to handle specific issues that

may arise, by providing review of the Privacy Officer's decision by the DHS Chief Privacy Officer, and, to the extent permitted by existing law, regulations, and policy, by allowing covered individuals access to their information and permitting them to challenge its completeness. Additionally, as an overarching mechanism to ensure appropriate privacy protections, US-VISIT operators will conduct periodic strategic reviews of the data to ensure that what is collected is limited to that which is necessary for US-VISIT purposes,

US-VISIT Increment 1 will store fingerprint images, both in the IDENT database and transiently on the some POE workstations and departure kiosks. These images are, of course, sensitive, and their storage could present a security as well as a privacy risk. Because retention of fingerprint images is functionally necessary so that manual comparison of fingerprints can be performed to verify biometric watch list matches, appropriate mitigation strategies will be utilized, including encryption on the departure kiosks and physical and logical access controls on the POE workstations and on the IDENT system.

The chart below shows, in tabular form, the privacy risks associated with US-VISIT, Increment One, and the mitigation efforts that will address these risks.

Privacy Threats and Mitigation Methods Detailed

Type of Threat	Description of Threat	Type of Measures to Counter/Mitigate Threat
Unintentional threats from insiders[3]	Unintentional threats include flaws in privacy policy definition; 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) developing 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).

[3] 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 and unintentional threats from authorized external entities[4]	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 routine use agreements 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, 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.

6. Summary and Conclusions

Legislation both before and after the events of September 11, 2001 led to the development of the US-VISIT Program. The program is based on Congressional concerns with visa overstays, the number of illegal foreign nationals in the country, and overall border security issues. Requirements for the program, including the implementation of an integrated and interoperable border and immigration management system, are embedded in various provisions of 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 U.S.A. PATRIOT Act, Public Law 107-56; and The Enhanced Border Security and Visa Entry Reform Act ("Border Security Act"), Public Law 107-173. As a result, many of the characteristics of US-VISIT were pre-determined. These characteristics include:

- Use of a National Institute of Standards and Technology (NIST) biometric standard for identifying foreign nationals;
- Use of biometric identifiers in travel and entry documents issued to foreign nationals, including the ability to read such documents at U.S. ports of entry;
- Integration of arrival/departure data on foreign nationals, including commercial carrier passenger manifests; and
- Integration with other law enforcement and security systems.

[4] These include individuals and systems which 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.

These and other requirements substantially constrained the high-level design choices available to the US-VISIT Program. A major choice for the program concerned whether to develop an entirely or largely new system or to build upon existing systems. Given the legislatively imposed deadline of December 31, 2003 for establishing an initial operating capability, along with the various integration requirements, the program opted to leverage existing systems—IDENT, ADIS, and the Passenger Processing Component of TECS.

As a result of this choice for Increment 1, DHS has determined that a new information system would not be created. Nevertheless, in order to effectively and accurately assess the privacy risks of US-VISIT, and because the program represents a new business process, this Privacy Impact Assessment was performed. In the process of conducting this PIA, DHS identified the need to (1) update the SORNs of the ADIS and IDENT systems to accurately reflect US-VISIT requirements and usage, which has been accomplished, and (2) examine the privacy and security aspects of the existing SORNs and implement any additional necessary strategies to ensure the privacy and security of US-VISIT data.

Based on this analysis, it can be concluded that

- Most of the high-level design choices for US-VISIT Increment 1 were statutorily pre-determined;
- US-VISIT Increment 1 creates a pool of individuals whose personal information is at risk; but
- US-VISIT Increment 1 mitigates specific privacy risks; and
- US-VISIT, through its own Privacy Officer and in collaboration with the DHS Chief Privacy Officer, will continue to track, assess, and address privacy issues throughout the life of the US-VISIT program and update this PIA to reflect additional increments of the program.

Contact Point and Reviewing Official

Contact Point: Steve Yonkers
US-VISIT Privacy Officer
(202) 298-5200

Reviewing Official: Nuala O'Connor Kelly
Chief Privacy Officer, DHS
(202) 772-9848

Comments

We welcome your comments on this privacy impact assessment. Please write to: Privacy Office, Attn.: US-VISIT PIA, U.S. Department Of Homeland Security, Washington, DC 20528, or email privacy@dhs.gov. Please include US-VISIT PIA in the subject line of the email.

Appendix

US-VISIT Program

Privacy Policy

What is the purpose of the US-VISIT program?

The United States Visitor Immigrant Status Indicator Technology (US-VISIT) is a United States Department of Homeland Security (DHS) program that enhances the country's entry and exit system. It enables the United States to record the entry into and exit out of the United States of foreign nationals requiring a visa to travel to the U.S., creates a secure travel record, and confirms their compliance with the terms of their admission.

The US-VISIT program's goals are to:

a. Enhance the security of American citizens, permanent residents, and visitors

b. Facilitate legitimate travel and trade

c. Ensure the integrity of the immigration system

d. Safeguard the personal privacy of visitors

The US-VISIT initiative involves collecting biographic and travel information and biometric identifiers (fingerprints and a digital photograph) from covered individuals to assist border officers in making admissibility decisions. The identity of covered individuals will be verified upon their arrival and departure.

Who is affected by the program?

Individuals subject to the requirements and processes of the US-VISIT program ("covered individuals") are those who are not U.S. citizens at the time of entry or exit or are U.S. citizens who have not identified themselves as such at the time of entry or exit. Non-U.S. citizens who later become U.S. citizens will no longer be covered by US-VISIT, but the information about them collected by US-VISIT while they were non-citizens will be retained, as will information collected about citizens who did not identify themselves as such.

What information is collected?

The US-VISIT program collects biographic, travel, travel document, and biometric information (photographs and fingerprints) pertaining to covered individuals. No personally identifiable information is collected other than that which is necessary and relevant for the purposes of the US-VISIT program.

How is the information used?

The information that US-VISIT collects is used to verify the identity of covered individuals when entering or leaving the U.S. This enables U.S. authorities to more effectively identify covered individuals that:

- Are known to pose a threat or are suspected of posing a threat to the security of the United States;
- Have violated the terms of their admission to the United States; or
- Are wanted for commission of a criminal act in the United States or elsewhere.

Personal information collected by US-VISIT will be used only for the purposes for which it was collected, unless other uses are specifically authorized or mandated by law.

Who will have access to the information?

Personal information collected by US-VISIT will be principally accessed by Customs and Border Protection, Immigration and Customs Enforcement, Citizenship and Immigration Services, and Transportation Security Officers of the Department of Homeland Security and Consular Officers of the Department of State. Others to whom this information may be made available include appropriate federal, state, local, or foreign government agencies when needed by these organizations to carry out their law enforcement responsibilities.

How will the information be protected?

Personal information will be kept secure and confidential and will not be discussed with, nor disclosed to, any person within or outside the US-VISIT program other than as authorized by law and in the performance of official duties. Careful safeguards, including appropriate security controls, will ensure that the data is not used or accessed improperly. In addition, the DHS Chief Privacy Officer will review pertinent aspects of the program to ensure that proper safeguards are in place. Roles and responsibilities of DHS employees, system owners and managers, and third parties who manage or access information in the US-VISIT program include:

1. DHS Employees

As users of US-VISIT systems and records, DHS employees shall:

- Access records containing personal information only when the information is needed to carry out their official duties.
- Disclose personal information only for legitimate business purposes and in accordance with applicable laws, regulations, and US-VISIT policies and procedures.

2. US-VISIT System Owners/Managers

System Owners/Managers shall:

- Follow applicable laws, regulations, and US-VISIT program and DHS policies and procedures in the development, implementation, and operation of information systems under their control.
- Conduct a risk assessment to identify privacy risks and determine the appropriate security controls to protect against the risk.
- Ensure that only personal information that is necessary and relevant for legally mandated or authorized purposes is collected.
- Ensure that all business processes that contain personal information have an approved Privacy Impact Assessment. Privacy Impact Assessments will meet appropriate OMB

and DHS guidance and will be updated as the system progresses through its development stages.

- Ensure that all personal information is protected and disposed of in accordance with applicable laws, regulations, and US-VISIT program and DHS policies and procedures.
- Use personal information collected only for the purposes for which it was collected, unless other purposes are explicitly mandated or authorized by law.
- Establish and maintain appropriate administrative, technical, and physical security safeguards to protect personal information.

3. Third Parties

Third parties shall:

- Follow the same privacy protection guidance as DHS employees.

How long is information retained?

Personal information collected by US-VISIT will be retained and destroyed in accordance with applicable legal and regulatory requirements.

Who to contact for more information about the US-VISIT program

Individuals whose personal information is collected and used by the US-VISIT program may, to the extent permitted by law, examine their information and request correction of inaccuracies. Individuals who believe US-VISIT holds inaccurate information about them, or who have questions or concerns relating to personal information and US-VISIT, should contact the Privacy Officer, US-VISIT Program, Department of Homeland Security, Washington, DC 20528. Further information on the US-VISIT program is also available at www.dhs.gov/us-visit.