US-VISIT Program, Increment 2
Privacy Impact Assessment

In Conjunction with the Interim Final Rule of August 31, 2004

September 14, 2004

US-VISIT

United States
Visitor and Immigrant Status Indicator Technology
Program Office

US-VISIT Program, Increment 2 (Including VWP)

Privacy Impact Assessment

1. Introduction

The United States Congress has directed the Executive Branch to establish an integrated entry and exit data system to accomplish the following[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 covered individuals with the terms of their admission into the United States.

The Department of Homeland Security (DHS) is complying with this congressional mandate through the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program.

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.

The first phase of US-VISIT, referred to as Increment 1, captured entry and exit information about nonimmigrant visitors whose records are not subject to the Privacy Act. Rather than establishing an entirely new information system, DHS integrated and enhanced 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 arising as a result of the program, DHS's Chief Privacy Officer directed that a Privacy Impact Assessment (PIA) be performed in accordance with the guidance issued by the Office of Management and Budget (OMB) on September 26, 2003, and that the PIA be updated as necessary to reflect future changes. This update of the initial PIA of January 4, 2003[2] is prompted by:

1. The inclusion of Visa Waiver Program (VWP) travelers in this entry and exit system;
2. The expansion of US-VISIT to the 50 busiest U.S. land border POEs; and

[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.

[2] The initial privacy impact assessment was published in the *Federal Register* of January 4, 2004, but was amended to correct a technical error (an incorrect telephone number) on January 16, 2004. See 68 FR 2608 (Jan. 16, 2004).

3. Changes in the business processes used by DHS to share information with Federal law enforcement agencies.

The principal impact of these changes is expansion of the pool of individuals subject to US-VISIT requirements and processes, and changes in the means of access used by DHS to share information with other law enforcement agencies.

2. System Overview

• What information is to be collected

Individuals subject to the principal data collection requirements and processes (including biometric collection and watch list checks) of the US-VISIT Program are nonimmigrant visa holders and VWP entrants traveling through air, sea, and the 50 busiest U.S. land border POEs. In addition, US-VISIT supports validation of the U.S.-issued travel documents of immigrant and nonimmigrant visa holders. Collectively, these constitute US-VISIT "covered individuals." DHS regulations and related regulatory actions published in the *Federal Register* further describe coverage of the program. Recent *Federal Register* publications describing US-VISIT include:

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

The information to be collected from these individuals may include 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 fingerprints. US-VISIT will capture and store this information using existing systems that record this information from travel documents and directly from covered individuals.)[3]

• 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 DHS, information is being collected about visitors to enhance national security while facilitating legitimate travel and trade. US-VISIT collects, maintains, and shares information in order to determine whether the individual:

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

[3] Individuals may have biometric identifiers captured to compare against biometrics on US-issued travel documents at the time of entry, but these identifiers are not stored and processed by US-VISIT.

- Can receive, extend, change, or adjust immigration status;
- Has overstayed or otherwise violated the terms of their admission;
- Should be apprehended or detained for law enforcement action; and
- Needs special protection/attention (e.g., Refugees).

- **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 any covered individual—including VWP individuals—will be contingent upon submission of the information required by US-VISIT, including biometric identifiers. A covered individual who declines to provide required biometrics is inadmissible to the United States.[4] An individual who declines to provide required biometrics may withdraw his or her application for admission, or be subject to removal proceedings. DHS has instituted procedures to process and admit individuals who are physically unable to provide the required biometrics.

US-VISIT has its own Privacy Officer to ensure that the privacy of all visitors is respected and to respond to individual concerns which have been or may be raised about the collection of the required information. Extensive stakeholder outreach and information dissemination activities are taking place, which are reviewed and adjusted on an ongoing basis to ensure maximum effectiveness. Further, the DHS Chief Privacy Officer, who serves as the appellate review authority for all individual complaints and concerns about the program, will exercise comprehensive oversight of all phases of the program to ensure that privacy concerns are respected throughout implementation.

3. System Architecture

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

1. The Arrival and Departure Information System (ADIS)[5]
2. The Passenger Processing Component of the Treasury Enforcement Communications System (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 2003)..

[6] System of Records Notice for Treasury Enforcement Communications System (TECS), TREASURY/CS.244, 63 FR 60809 (December 1998): 60809. 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 U.S. 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 that they support, are (1) Interagency Border Inspection System (IBIS) (including the Nonimmigrant visa (NIV) database), supporting the lookout process; and

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

US-VISIT Increment 1 involved modification and extension of client software on POE workstations (which include other functionality that is not part of US-VISIT) and the development of departure devices to collect exit data. Under Increment 2, this POE workstation functionality will be extended to workstations at the relevant land border POEs along with the ability to print Arrival/Departure Record Form I-94[8] departure stubs based on captured data and to transfer that data to a non-US-VISIT component of TECS for forwarding to the Nonimmigrant Information System[9] (NIIS).[10]

Workstations at all POEs will have the ability to perform biometric comparisons (stored photo vs. travel document photo vs. traveler) and document authentication on U.S. travel documents issued to non-citizens (visas in the case of US-VISIT). Several different approaches to departure devices for air and sea ports are currently being tested[11] and will be analyzed in a future PIA. This PIA considers departure devices only in general terms.

The changes to ADIS, TECS, and IDENT for Increment 1 included:

1. Modifications to TECS to give immigration inspectors the ability to display nonimmigrant-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 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 or extensions in the status of individuals from two other databases—the Student and Exchange Visitor Information System (SEVIS) and the Computer Linked Application Information Management System (CLAIMS 3) to ADIS.

The changes to these systems for Increment 2 include:

1. Modification of existing workstations in the Passport Control areas of land POEs to capture biographic and biometric information.

---

(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 2003).

[8] Form I-94 and its variants must be filled out by most foreign visitors to the U.S.

[9] System of Records Notice for Nonimmigrant Information System (NIIS), JUSTICE/INS-036, 68 FR 5048-5049 (January 2003).

[10] This supports a previously existing business process by providing more efficient data entry. Previously, all I-94 data was manually entered into NIIS and then replicated in a non-US-VISIT component of TECS. The information entered at the POEs will flow into this component of TECS and be replicated in NIIS.

[11] Department of Homeland Security; Border and Transportation Security; Notice to Aliens Included in the United States Visitor and Immigrant Status Indicator Technology System (US–VISIT), 69 FR 46556-46558 (August 3, 2004).

2. Establishment of an interface between the land border POE workstations and a non-US-VISIT component of TECS to support forwarding of I-94 information to NIIS.
3. Changes in the business process DHS uses to share information with other Federal law enforcement agencies.

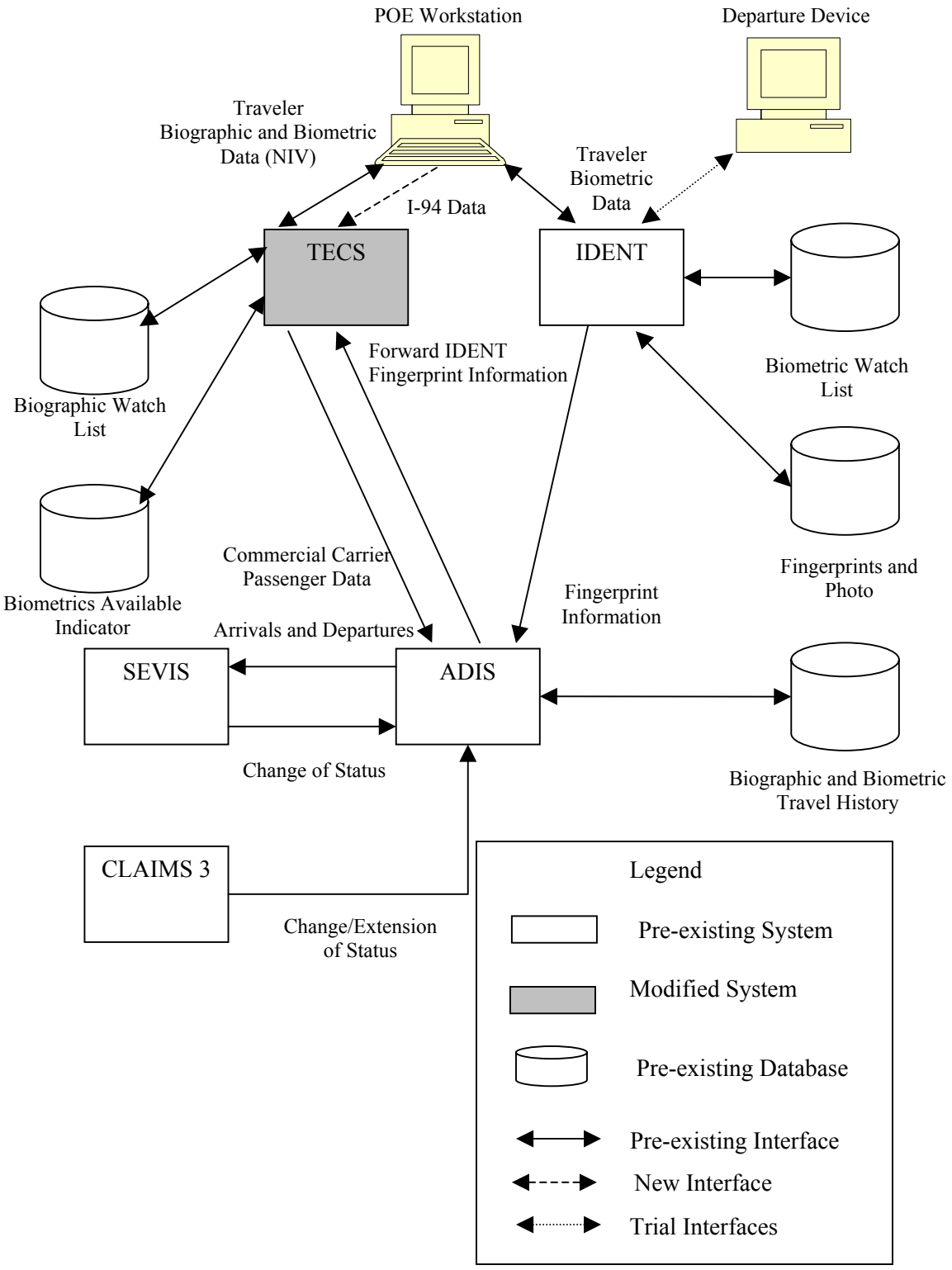
US-VISIT interfaces with other, non-DHS systems for relevant purposes, including watch list updates and checks. In particular, US-VISIT exchanges biographic and biometric information with the State Department's Consular Affairs Consolidated Database (CCD) as part of the visa application process (CCD does not retain any biometric information.)

As stated in the PIA for US-VISIT Increment I, which was published on the DHS website and in the Federal Register on January 4, 2004[12], the US-VISIT program shares information with federal, state, local, tribal, and foreign law enforcement agencies. This information sharing enhances the ability of DHS and other law enforcement agencies to work more cooperatively and effectively in achieving their national security and law enforcement objectives. In order to enhance the effectiveness of the FBI's access of US-VISIT information, US-VISIT is modifying the method by which it shares information by providing the FBI with direct access. Memoranda of Understanding establishing limits on access, use, disclosure and disposition will be put in place to strictly govern these interfaces in order to minimize any privacy impacts.

[12] A technical correction was published on January 16, 2004.

The diagram below presents data flows in the context of the high-level system architecture. Note that the terms "pre-existing," "modified," and "new" are relative to US-VISIT Increment 1.

Figure 1: US-VISIT Increment 2 Architecture



- **Intended use 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 existing database systems, DHS is 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 enables DHS to protect U.S. borders and national security through improved immigration control. US-VISIT will also help DHS prevent aliens from obtaining benefits to which they are not entitled. As announced previously, DHS also shares information obtained through US-VISIT with other federal, state, local, tribal, and foreign law enforcement partners to accomplish common goals.

4. Administrative Controls on Access to the Data

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

The personal information collected and maintained by US-VISIT is accessed by employees of DHS components—Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and United States Citizenship and Immigration Services (USCIS) – and the Department of State for immigration and border management purposes.

The information also is accessed by agents of the Federal Bureau of Investigation (FBI) for law enforcement purposes and 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 Privacy Act System of Records Notices (SORNs) 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. Any disclosure by DHS must be compatible with the purpose for which the information was collected. Any non-DHS agency granted access to this information will sign a Memorandum of Understanding that will govern protection and usage of the information.

- **How the information will be secured**

The US-VISIT Program secures information and the systems on which that information resides by complying with the requirements of the DHS Information Technology (IT) Security Program Handbook. This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, 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, TECS, and IDENT have been individually certified as satisfying the applicable security requirements of their legacy (pre-DHS) organizations and will undergo recertification as required by law and DHS policy.

One aspect of the DHS comprehensive program to provide information security involves the establishment of strict rules of behavior for each major application, including US-VISIT. These rules of behavior require all users to be adequately trained regarding the security of their

systems. These rules also require a periodic assessment of physical, technical, and administrative 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.

5. Information Life Cycle and Privacy Impacts

The table below provides an overview of the privacy risks associated with US-VISIT and the types of mitigation measures that address those risks.

Table 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[13]	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[14]	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	These threats are addressed by technical safeguards (in particular, boundary controls such as firewalls) and administrative safeguards in the form of 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.

[13] 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.

[14] 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.

	errors made by custodians	
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.

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.[15] US-VISIT has developed and is publishing its own set of privacy principles, which will be used for this analysis in all future PIAs.

- **Collection**

US-VISIT collects, uses, and retains only the personal information necessary for its purposes. As a result of the Arrival/Departure Record Form I-94 data capture process, Increment 2 does collect data elements not already collected by US-VISIT, but only in support of an existing business process and system of records. All these data are transferred to a non-US-VISIT component of TECS that replicates the data in NIIS and forwards these data to NIIS. None of the I-94 data is used or retained by US-VISIT. This represents a minor change to an existing (non-US-VISIT) data collection process. Currently, Forms I-94, I-94W, and I-94T are completed by hand, collected, manually reviewed for legibility and accuracy, and sent to a data entry contractor for entry into NIIS. US-VISIT will streamline this process for Form I-94 at applicable land POEs by electronically capturing I-94 data. (The process for Forms I-94W and I-94T remains unchanged.) Moreover, the Form I-94 departure stub will be printed for issuance to the traveler as evidence of the terms of admission. This affords individuals at these POEs the opportunity to verify that their I-94 information was properly entered by the CBP official and to request correction of any inaccuracies at the time of departure—an additional integrity safeguard.

[15] 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.

Otherwise, the expansion of US-VISIT to land border POEs provides for the same data collection that Increment 1 implemented at air and sea POEs, with identical risks and mitigations. Similarly, the inclusion of VWP countries, while expanding the pool of covered individuals, does not qualitatively affect the risk analysis.[16] The biometric comparison and document authentication process to which immigrant visa holders (in addition to other covered individuals) may be subjected further expands the pool of covered individuals, but in a more limited fashion and, again, with no qualitative impact on the risk analysis.

While US-VISIT does not constitute a new system of records, it does expand the types of data held in its component systems. (The component SORNs were previously updated to reflect US-VISIT usage.) By definition this creates a general privacy risk. This risk is mitigated, however, 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, and ongoing consultation with stakeholders and representative organizations. Additionally, US-VISIT will conduct periodic strategic reviews of the data to ensure that what is collected is limited fundamentally to that which is necessary for US-VISIT purposes.

- **Use and Disclosure**

The IDENT and TECS systems collect data that are used for purposes other than those identified by US-VISIT. This presents a potential notice risk. This risk is mitigated in several ways. First, US-VISIT isolates US-VISIT data from non US-VISIT data on component systems. US-VISIT transactions have a unique identifier to differentiate them from other TECS and IDENT transactions. This allows for improved oversight and audit capabilities to ensure that the data are being handled in a manner consistent with all applicable federal laws and regulations regarding privacy and data integrity. All users receive specific privacy and security training on the handling of this data, including any special restrictions on data use and/or disclosure such as those resulting from any applicable international agreements and special types of status (e.g., asylum applicants). Second, the IDENT and TECS systems have their own published SORNs, which explain permissible data uses for both US-VISIT and non-US-VISIT purposes. This too mitigates the risk of individuals not having received effective notice. Third, Memoranda of Understanding and of Agreement are being put into place with third parties (including other agencies, such as the FBI and the Department of State,) to address privacy protections and use limitations for US-VISIT data.

- **Processing**

The data flows, which occur over an encrypted network between US-VISIT component systems and/or applications, are limited and confined only to those transactions 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

[16] The air Passenger Name Record (PNR) data covered by a data-sharing agreement between the U.S. and the European Union are not used by US-VISIT.

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 is also being used to identify any problem trends in the matching process (e.g. compounded errors) and implement risk mitigation as needed (e.g., special checks targeted at specific data elements exhibiting a statistically significant tendency to cause matching errors).

Matching errors are also a potential issue at POEs. The matching errors and the integrity risk they constitute can be of two main types: 1) watch list false positive (where an individual is incorrectly matched to someone on a watch list) and 2) incorrect 1:1 verification mismatch (where a false discrepancy is detected between an individual and their own records). POE mismatch rates to date appear to be consistently low for erroneous watch list hits (a cumulative rate of less than 0.1%). Both types of risk are substantially mitigated by on-the-spot manual verification and clearance (taking an average of around 3 minutes for watch list false positives) combined with the US-VISIT redress policy.

US-VISIT has implemented a three-stage 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. US-VISIT will refine this process on an ongoing basis through systematic consideration of specific scenarios, including expedited removal.

- **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 varied 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 integrity/security, access, and/or redress risk as personal information could disappear from one or more component systems while persisting in others. In order to most appropriately and effectively mitigate these risks, a comprehensive assessment of retention requirements is currently being conducted. When complete, this assessment will be used to establish a uniform retention policy for personal information collected by US-VISIT. It includes consideration of any applicable international agreements or special types of status, as described above, as well as consideration of issues related to retention of personal data for individuals who are covered by US-VISIT and later become either legal permanent residents or U.S. citizens. Additional mitigation is provided on a case-by-case basis by the US-VISIT redress process, which will complement the uniform retention policy that is under development.

US-VISIT stores fingerprint images, both in the IDENT database and temporarily on some POE

workstations before transferring them to IDENT. These images are 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 are utilized, including physical and logical access controls on the POE workstations and on the IDENT system.

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

Legislation both before and after the events of September 11, 2001, led to the development of the US-VISIT Program. The program 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 added urgency to development and deployment of this Program. Requirements for the program, including the implementation of an integrated and interoperable border and immigration management system, are embedded in various provisions of: 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 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, among others:

- 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, and the ability to read such documents at U.S. POEs;
- Integration of arrival/departure data on foreign nationals, including commercial carrier passenger manifests; and
- Integration with other law enforcement and security systems.

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 determined that a new system of records would not be created. US-VISIT Increment 1 integrated and enhanced the capabilities of existing systems; it did not create a new system of records outside of the records that exist on other systems. (These systems have been modified to support US-VISIT functionality—as described in Section 3—and their SORNs have been revised accordingly.) Although Increment 2 has not altered this assessment, US-VISIT is studying whether creation of a unique system of records would enhance privacy protections.

7. Summary and Conclusions

In order to assess the privacy risks of US-VISIT effectively and accurately, and because the program represents a new business process, the initial PIA was carried out and performed in accordance with OMB guidelines. In the process of conducting the PIA for Increment 1, 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 on an ongoing basis any necessary additional strategies to ensure the privacy and security of US-VISIT data. Under Increment 2, the coverage of US-VISIT is expanded to include additional categories of visitors, additional ports of entry, and changed business processes by which information is shared outside DHS. These changes have been made in ways that ensure strong privacy controls and oversight.

Based on these analyses, it can be concluded that

- Most of the high-level design choices for US-VISIT were statutorily pre-determined;
- US-VISIT creates a pool of individuals whose personal information is at risk (covered individuals), which Increment 2 expands; but
- US-VISIT mitigates specific privacy risks and Increment 2 does not create a need for new mitigations; and
- US-VISIT through its 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.

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 U.S.A. PATRIOT Act

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

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.

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

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

Department of Homeland Security; United States Visitor and Immigrant Status Indicator Technology Program (''US–VISIT''); 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).

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

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

ICE Security Requirements, printed October 30, 2003.

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

Increment 2B Business Requirements, Version 0.5, US-VISIT, undated.

Increment 2B Concept of Operations, Version 2.2, US-VISIT, April 29, 2004.

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

IT Security Program Handbook, Version 1.3, Sensitive Systems, Department of Homeland Security, ID-4300A, June 20, 2003.

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 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.

Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach, Commission of the European Communities, December 16, 2003.

Appendix B: List of Acronyms

ADIS	Arrival 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
DD	Departure Device
DHS	Department of Homeland Security
DMIA	Data Management Improvement Act
DoB	Date of Birth
DocKey	Document Key
DoS	Department of State
FBI	Federal Bureau of Investigation
FIN	Fingerprint Identification Number
FOIA	Freedom of Information Act
FRD	Functional Requirements Document
I&A	Identification and Authentication
IAFIS	Integrated Automated Fingerprint 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
NATO	North Atlantic Treaty Organization
NIIS	Nonimmigrant Information System
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
PNR	Passenger Name Record
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
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

Appendix C: Data Flows Detailed

Pursuant to Public Law 107-173, Veterans Affairs and Housing and Urban Development and Independent Agencies Appropriations Act of 2002, US-VISIT information is and will be integrated with other DHS databases and data systems. US-VISIT information is and 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), the Nonimmigrant Information System (NIIS), and the State Department's Consular Affairs Consolidated Database. However, US-VISIT information is logically separated from other data and users on the component systems (TECS, IDENT, and ADIS).

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 is being used by individual US-VISIT processes 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
	  ○ Type
	  ○ Number
	  ○ Date of issuance
	  ○ Country of issuance
	• Fingerprint Identification Number (FIN)
	• Biographic and biometric watch list hit/match[17]

Admission data	• Class of admission • Admit until date

Visa data	• First name
	• Last name
	• Visa
	  ○ Class
	  ○ Number
	  ○ Entry (multiple or one time entry)
	  ○ Issuance date
	  ○ Expiration date
	• Passport type
	• Passport number
	• Gender
	• Date of birth
	• Nationality

Travel document data	Dependent on document type but will include
	• Complete name
	• Document
	  ○ Number
	  ○ Date of issuance
	  ○ Country of issuance

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

Table C-1: Data Aggregates (continued)

Aggregate Name	Data Elements

Passenger manifest	• Complete name
	• Date of birth
	• Gender
	• Document
	  ○ Country of issuance
	  ○ Type
	  ○ Number
	  ○ Expiration date
	  ○ 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

Aggregate Name	Data Elements

Visa application	• State Department case ID
	• Applicant ID
	• Complete name
	• Gender
	• Date of birth
	• Country of birth
	• Nationality
	• Passport
	  ○ Number
	  ○ Type
	  ○ Date of issuance
	  ○ Country of issuance
	  ○ City of issuance
	  ○ Expiration date
	• Visa type
	• Visa class

Encounter data	• Encounter date and time
	• Encounter applicant ID
	• Travel document
	  ○ Type
	  ○ Country of issuance
	  ○ 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 Increment 2 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, fingerprints, biographic data (watch list updates)	DocKey (including biometric watch list hit/match), fingerprints, 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[18], 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, fingerprints, admission data, I-94 data	Updated passenger manifest, DocKey, photo, fingerprints, admission data, I-94 data
Departure Device	TBD pending exit pilot evaluation	TBD pending exit pilot evaluation
Candidate Verification Tool (CVT)	Candidate & subject fingerprints, FINs, photos, verification history	Verification decision
Secondary Web Tool	Encounter data, FIN (previous encounter)	

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

Table C-3: US-VISIT Increment 2 Processes and Data Usage

Process	Subprocess	System/Application	Data Usage
Pre-Arrival	Visa application check	TECS, IDENT	Visa application, photo, fingerprints, 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, fingerprints
	Biometric watch list check	IDENT, Workstation	DocKey, fingerprints
	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 Web 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, Departure Device	DocKey, fingerprints
	Biometric watch list check	IDENT, Departure Device	DocKey, fingerprints

Table C-3: US-VISIT Increment 2 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 fingerprints, FINs, photos, verification history
Audit log capture		TECS, IDENT, ADIS	User, date and time, system actions

Table C-4: US-VISIT Increment 2 System/Application Interface Data Flows[19]

From/To	W/S	TECS	IDENT	ADIS	DD	SWT	CVT	SEVIS	CLAIMS 3	DOJ IAFIS	CCD	NUSV TECS
Work-Station (W/S)		DocKey, admission data, updated passenger manifest	DocKey, photo, finger-prints									I-94 data
TECS	DocKey, admission data, visa data (NIV), photo (NIV), passenger manifest, status			DocKey, passenger manifest, admission data								
IDENT	DocKey			DocKey	TBD	Encounter data, complete name, gender, DoB, doc type, number, and country of issuance, FIN (previous encounter)	Candidate & subject fingerprints, FINs, photos, verification history				Encounter data, watch list hits	
ADIS		DocKey						Complete				

19 Note: Only selected third_party interfaces are shown; for all potential third parties, see the component SORNs.

From/To	W/S	TECS	IDENT	ADIS	DD	SWT	CVT	SEVIS	CLAIMS 3	DOJ IAFIS	CCD	NUSV TECS
								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				
Departure Device (DD)			TBD									
Secondary Web Tool (SWT)												
Candidate Verification Tool (CVT)			Verification decision									
SEVIS				Complete name, DoB, gender, nationality, visa type, visa number,								

From/To	W/S	TECS	IDENT	ADIS	DD	SWT	CVT	SEVIS	CLAIMS 3	DOJ IAFIS	CCD	NUSV TECS
				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/req								

From/To	W/S	TECS	IDENT	ADIS	DD	SWT	CVT	SEVIS	CLAIMS 3	DOJ IAFIS	CCD	NUSV TECS
				uested)								
Dept. of Justice (DOJ) IAFIS			Fingerprints, 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												

Appendix D: Safeguards 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 4.2.1 above.

The table below provides greater detail on the various physical and electronic measures employed to counter the various threats to US-VISIT Increment 2. Compliance of ADIS, the Passenger Processing Component of TECS, IDENT and the POE workstations with ID-4300A, the BLSR, and the DHS Physical Security Handbook is assumed. As reflected in the table, many different threats can be mitigated by the same safeguards.

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 entrée by unauthorized entities.
Intentional physical threats from 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 entrée by unauthorized entities.
Intentional physical threats from external entities	POE Workstation	Physical protection	Physical controls may be specific to each POE. Assumed to be in compliance with BLSR and ID-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). Issue to be addressed during system integration: Define procedures for correlation among different user identifiers (issued by PICS and the legacy mechanisms in ADIS, the Passenger Processing

[20] 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 component provide user ID / password mechanisms. The US-VISIT, Increment 1 Functional Requirements Document (FRD) states that "The Password Issuance Control System shall be used for user identification and password management." System integration must address the issue of whether these password mechanisms will be integrated to provide a single sign-on capability or whether separate logon processes

Nature of Threat	Architectural Placement	Safeguard	Mechanism
			Component of TECS, IDENT, and the POE workstations) to facilitate tracking and investigation of activities by individual users. [20]
Intentional and unintentional electronic threats from authorized (internal and external) entities	ADIS	Technical protection: I&A	User identifier and password
Intentional and unintentional electronic threats from authorized (internal and external) entities	IDENT	Technical protection: I&A	User identifier and password
Intentional and unintentional electronic threats from authorized (internal and external) entities	Passenger Processing Component of TECS	Technical protection: I&A	User identifier and password
Intentional and unintentional physical and electronic threat from unauthorized external entities	POE Workstation	Technical protection: I&A	User identifier and password. US-VISIT, Increment 2 client software runs on Windows 2000 workstations connected to the DHS network.
Intentional and unintentional electronic threats from	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	POE Workstation	Technical protection: Authorization and	Access to US-VISIT client applications is authorized, given that access to the

will be used (e.g., logon to POE Workstation and/or the DHS network, logon to IBIS client, logon to IDENT client). If separate logons are involved, technical or procedural controls will be needed to ensure that actions taken by a single user can be correlated and traced to that user. Alternatives will be defined and evaluated as part of the system integration process. It is anticipated that the issue will be resolved so as to ensure compliance with the Baseline Security Requirements (BLSR). A solution that provides adequate security will address the privacy concern.

Nature of Threat	Architectural Placement	Safeguard	Mechanism
physical and electronic threat from unauthorized external entities		access control	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 ID-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, below.[21]
Intentional physical and electronic threats from external entities	POE Workstation, Departure Device	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	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

[21] Some Port of Entry (POE) workstations and future point of departure devices will store various personal information, if only transiently.

The Consolidated Functional Requirements Document, Section 5.3, specifies that the departure devices will store subject biographic and biometric data when communication between departure devices and the IDENT database is unavailable. Depending on volume and length of communication outage, this could leave potentially large amounts of personal information residing on these devices. Particularly because the departure devices are intended to be self-service, this poses a significant privacy risk. It is believed that data will be encrypted on the departure devices to mitigate this risk.

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.

It is anticipated that these issues will be resolved so as to ensure compliance with the DHS/ICE BLSR for Automated Information Systems. A solution that provides adequate security for the POE workstations and departure devices will address the privacy concerns.

Nature of Threat	Architectural Placement	Safeguard	Mechanism
	Component of TECS, ADIS, and IDENT)		future capability for additional protection of the privacy of US-VISIT transactions.
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 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? • 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 are 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	Not available for this version of the PIA.