United States Government Accountability Office

GAO

Report to the Chairman and Ranking Member, Committee on Homeland Security, House of Representatives

February 2008

HOMELAND SECURITY

Strategic Solution for US-VISIT Program Needs to Be Better Defined, Justified, and Coordinated

G A O
Accountability ★ Integrity ★ Reliability

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-08-361, a report to the Chairman and Ranking Member, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

The Department of Homeland Security's (DHS) U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program's goals are to enhance the security of U.S. citizens and visitors, facilitate legitimate travel and trade, ensure the integrity of the U.S. immigration system, and protect the privacy of visitors. It is to use biometric and biographic information to control and monitor the pre-entry, entry, status, and exit of foreign visitors. GAO was asked to determine (1) whether DHS has defined and economically justified a strategic solution for meeting US-VISIT goals; (2) the biometric technology options DHS has considered and the basis for the selected options; and (3) DHS's efforts to define, manage, and coordinate the relationships between US-VISIT and other immigration and border management programs. To accomplish this, GAO assessed key program documentation against relevant criteria and examined available biometric research.

What GAO Recommends

GAO is recommending that the Secretary of Homeland Security ensure that the strategic solution components are well-defined and economically justified before investing large sums of money and that they are effectively coordinated with related programs. DHS concurred with GAO's recommendations and stated that it has initiated actions to implement them.

To view the full product, including the scope and methodology, click on GAO-08-361. For more information, contact Joel C. Willemssen at (202) 512-6222 or willemssenj@gao.gov.

February 2008

HOMELAND SECURITY

Strategic Solution for US-VISIT Program Needs to Be Better Defined, Justified, and Coordinated

What GAO Found

DHS has partially defined a strategic solution for meeting US-VISIT's goals. In particular, the US-VISIT program office has defined and begun to develop a key capability known as "Unique Identity," which is to establish a single identity for all individuals who interact with any immigration and border management organization by capturing the individual's biometrics, including 10 fingerprints and a digital image, at the earliest possible interaction. However, the program office has yet to define and economically justify a comprehensive strategic solution for controlling and monitoring the exit of foreign visitors, which is critical to accomplishing the program's goals. Further, the department did not economically justify its ongoing investment in Unique Identity in a timely fashion. Specifically, the program office did not justify its investment until about 14 months after selecting and pursuing an alternative solution and obligating about $65 million. The absence of a fully defined strategic solution and timely economic justification hinders informed decision making about the best course of action for accomplishing strategic program goals and inhibits the ability to measure performance and promote accountability.

DHS considered various biometric technologies, including fingerprints, facial, and iris technologies, and continues to use fingerprints as its foundational biometric technology. The focus on fingerprint technology is appropriate, given the opportunity to leverage existing DHS and Federal Bureau of Investigation identification systems and databases and to establish a single identity mechanism for all immigration and border management programs. In addition, research into fingerprints and other forms of biometric identification, such as facial recognition and iris scanning, show that fingerprints continue to be the most accurate biometric for identification purposes.

DHS is taking a range of evolving actions, primarily at the department level, to coordinate relationships among US-VISIT and other immigration and border management programs. Thus far, this evolution has yet to progress to the point of reflecting the full scope of key practices that GAO has previously identified as essential to enhancing and sustaining collaborative efforts that span multiple organizations. To its credit, the department has defined common outcomes through its strategic plan and enterprise architecture and has taken steps to implement other collaboration practices, such as leveraging resources across its screening programs and developing screening performance indicators. However, the US-VISIT program office has yet to fully define its relationships with other immigration and border management programs. As a result, the department is at increased risk of introducing the inefficiencies and reduced effectiveness that result from suboptimizing how these programs collectively support its immigration and border management goals and objectives.

Contents

Figures

Abbreviations

ADIS	Arrival Departure Information System
APIS	Advance Passenger Information System
BioVisa	Biometric Visa Program
BCC	Border Crossing Card
CBP	U.S. Customs and Border Protection
CCD	Consular Consolidated Database
CLAIMS 3	Computer Linked Application Information Management System
DHS	Department of Homeland Security
DOJ	Department of Justice
DMIA	Immigration and Naturalization Service Data Management Improvement Act of 2000
EA	enterprise architecture
EAB	Enterprise Architecture Board
ESB	Enterprise Service Bus
FBI	Federal Bureau of Investigation
GES	Global Enrollment System
IAFIS	Integrated Automated Fingerprint Identification System
ICE	U.S. Immigration and Customs Enforcement
iDSM	interim Data Sharing Model
IDENT	Automated Biometric Identification System
IIRIRA	Illegal Immigration Reform and Immigrant Responsibility Act of 1996
ISRS	Image Storage Retrieval System
IT	information technology
NIST	National Institute of Standards and Technology
POE	port of entry
RFID	radio-frequency identification
SCO	Screening Coordination Office
SBI	Secure Border Initiative
SEVIS	Student and Exchange Visitor Information System
TECS	Treasury Enforcement Communications Systems
US-VISIT	U.S. Visitor and Immigrant Status Indicator Technology
USCG	U.S. Coast Guard
USCIS	U.S. Citizenship and Immigration Services
WHTI	Western Hemisphere Travel Initiative

G A O
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

February 29, 2008

The Honorable Bennie G. Thompson
Chairman
The Honorable Peter T. King
Ranking Member
Committee on Homeland Security
House of Representatives

For many years the Congress and the administration have sought better ways to record and track the arrival and departure of foreign visitors through U.S. air, sea, and land ports of entry (POE). Pursuant to a series of statutory mandates,[1] the Department of Homeland Security (DHS), in concert with the Department of State, established a program to use biometric and biographic information to control and monitor the pre-entry, entry, status, and exit of foreign visitors.[2] This program, which is called the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program, is intended to enhance the security of U.S. citizens and visitors, facilitate legitimate travel and trade, ensure the integrity of the U.S. immigration system, and protect the privacy of visitors to the United States.

DHS has pursued US-VISIT in a series of four increments, with Increments 1 through 3 focusing on the near-term integration of existing systems, and Increment 4 intended to be a more strategic solution. As of February 2008, Increments 1 through 3 are completed, resulting in an entry capability that has been deployed and is operating at about 300 air, sea, and land POEs.

Because of the strategic importance of US-VISIT to our nation's evolving immigration and border management process, you asked us to determine (1) whether DHS has defined a strategic solution for meeting US-VISIT goals and whether the solution has been economically justified; (2) the biometric technology options DHS has considered and the basis for the selected options; and (3) DHS's efforts to define, manage, and coordinate the relationships between US-VISIT and other immigration and border

[1] Applicable statutes are described in detail in appendix II.

[2] Prior to the creation of DHS in 2002, the Immigration and Naturalization Service of the Department of Justice performed this mission.

management programs. To accomplish our objectives, we reviewed key program documentation, including plans and analyses, and compared them with relevant criteria. We also examined available government research on biometric technology options and compared efforts taken to coordinate the efforts of different organizational entities involved in US-VISIT with published coordination best practices. We conducted our review from January 2007 through January 2008, in accordance with generally accepted government auditing standards. Further details of our objectives, scope, and methodology are included in appendix I.

Results in Brief

DHS has partially defined a strategic solution for meeting US-VISIT program goals. In particular, the program office has defined and begun to develop one of the two key components of its strategic solution known as Unique Identity, which is to establish a single identity for all individuals who interact with any immigration and border management organization by capturing the individual's biometrics, including 10 fingerprints and a digital image, at the earliest possible interaction. However, the program office has yet to define and economically justify the second primary component of its strategic solution—exit, which is critical to accomplishing the program's goals. Compounding this is the lack of timely economic justification for the Unique Identity solution. For example, the program office did not economically justify its investment in Unique Identity until about 14 months after selecting and pursuing an alternative solution and obligating about $65 million. The absence of a fully defined strategic solution and timely economic justification hinders informed decision making about the best course of action for accomplishing strategic program goals and inhibits the ability to measure performance and promote accountability.

DHS considered various biometric technologies, including fingerprints, facial, and iris technologies, and continues to use fingerprints as its foundational biometric. The focus on fingerprint technology is appropriate, given the opportunity to leverage existing DHS and Federal Bureau of Investigation (FBI) identification systems and databases, and to establish a single identity mechanism for all immigration and border management programs. Further, research into fingerprints and other forms of biometric identification, such as facial recognition and iris scanning, show that fingerprints continue to be the most accurate biometric for identification purposes. Going forward, the program office is taking steps to permit it to introduce other biometric solutions at some future point.

DHS is taking a range of evolving actions, primarily at the department level, to coordinate relationships among US-VISIT and other immigration and border management programs, such as the Secure Border Initiative (SBI) and the Western Hemisphere Travel Initiative (WHTI). Specifically, the department has defined common outcomes through its strategic plan and enterprise architecture (EA), and has taken steps to implement other collaboration practices, such as leveraging resources across its screening programs and developing screening performance indicators. However, these actions do not yet reflect the full scope of key practices that we have previously identified as essential to enhancing and sustaining collaborative efforts that span multiple organizations. For example, the US-VISIT program office has yet to fully define either its relationships with WHTI and SBI*net* or its approaches relative to addressing outcomes shared by all three programs. As a result, the department risks suboptimizing how these programs collectively support its immigration and border management goals and objectives.

We are making recommendations to the Secretary of Homeland Security to ensure that the strategic solution components are well-defined, economically justified before investing large sums of money, and effectively coordinated with related programs. In written comments on a draft of this report, signed by the Director, Departmental GAO/Office of Inspector General Liaison, the department stated that it generally agreed with our observations and concurred with our recommendations, and that it has initiated actions to implement our recommendations. DHS also provided technical comments, which we have incorporated into this report as appropriate.

Background

US-VISIT's goals are to (1) enhance the security of U.S. citizens and visitors, (2) facilitate legitimate travel and trade, (3) ensure the integrity of the U.S. immigration system, and (4) protect the privacy of visitors. The program is to achieve these goals by

- collecting, maintaining, and sharing information on certain foreign nationals who enter and exit the United States;
- identifying foreign nationals who (1) have overstayed or violated the terms of their visit; (2) can receive, extend, or adjust their immigration status; or (3) should be apprehended or detained by law enforcement officials;

- detecting fraudulent travel documents, verifying visitor identity, and determining visitor admissibility through the use of biometrics (digital fingerprints and a digital photograph); and
- facilitating information sharing and coordination within the immigration and border management community.

Federal Statutes Provide a Strategic Framework for US-VISIT

A series of statutes, dating back to more than a decade ago, have provided a framework for the strategic focus of US-VISIT. A brief summary of statutes is provided below, and additional detail is provided in appendix II.

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA)[3] required the Attorney General to develop an automated system to record the departure of every foreign national from the United States and then match it to the individual's arrival record. Subsequently, section 2 of the Immigration and Naturalization Service Data Management Improvement Act (DMIA) of 2000[4] amended the original entry-exit provisions of the IIRIRA and required the Attorney General[5] to implement an integrated entry and exit data system for foreign nationals.[6] More specifically, the act required an electronic system that would provide access to and integrate foreign national arrival and departure data that are authorized or required to be created or collected under law and are in an electronic format in Department of Justice (DOJ) or Department of State databases, such as those used at POEs and consular offices. The system, as described in DMIA, is to compare available arrival records with available departure records, allow online search procedures to identify foreign nationals who may have overstayed their authorized period of admission, and use available data to produce a report of arriving and departing foreign nationals. DMIA also required the implementation of the system at airports and seaports by December 31, 2003, at the 50 highest volume land POEs by December 31, 2004, and at all remaining POEs by December 31, 2005.

[3] Pub. L. No. 104-208, div. C, sec. 110 (Sept. 30, 1996).

[4] 8 U.S.C. § 1365a.

[5] Effective March 1, 2003, the Immigration and Naturalization Service became part of DHS.

[6] On April 29, 2003, the Secretary of DHS renamed the entry-exit system the US-VISIT system.

Subsequent laws added specific biometric requirements to US-VISIT. The USA PATRIOT Act,[7] as amended, required the development and certification of a technology standard by January 26, 2003, including appropriate biometric identifiers that can be used to verify the identity of persons applying for a U.S. visa or seeking to enter the United States pursuant to a visa, for the purposes of conducting background checks, confirming identity, and ensuring that a person has not received a visa under a different name. The act also required DHS and the Department of State to focus on the utilization of biometric technology and the development of tamper-resistant documents readable at POEs for the integrated entry and exit data system. Additionally, the act required that a report be made to the Congress on the feasibility of enhancing the FBI's Integrated Automated Fingerprint Identification System (IAFIS) database and other identification systems in order to better identify aliens who may be wanted in connection with criminal investigations prior to the issuance of visas or entry into the United States.

The Visa Waiver Permanent Program Act[8] required DHS to develop and implement a fully automated system to control entry and exit of aliens at airports and seaports who enter the United States under the Visa Waiver Program. It also required that, by October 1, 2002, inspectors at POEs have access to Department of State and DHS information to determine whether an alien seeking a waiver under the program is eligible to be admitted into the United States or to receive a visa. Further, the act required that visa waiver applicants be checked against watch list systems and that, by October 1, 2003, aliens applying for a visa waiver have a machine-readable passport.[9] The act was subsequently amended to require, not later than August 3, 2008, an exit system using biometric information and recording

[7] 8 U.S.C. § 1379. USA PATRIOT Act stands for the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. As applicable here, the Act's requirements for the Immigration and Naturalization Service were taken over by DHS.

[8] Pub. L. No. 106-396 (Oct. 30, 2000).

[9] Between October 1, 2003, and September 30, 2007, the Secretary of State could waive the requirement for machine-readable passports if the country (1) was making progress toward ensuring that machine-readable passports are generally available to its nationals and (2) it has taken appropriate measures to protect against misuse of passports it issued that do not meet the requirements.

the departure on a flight leaving the United States of every alien participating in the Visa Waiver Program.[10]

The Enhanced Border Security and Visa Entry Reform Act of 2002[11] required DHS, in consultation with the Department of State, to use the technology standard, including biometric identifier standards developed under the USA PATRIOT Act, at POEs by October 26, 2005,[12] to install equipment and software at all POEs to allow biometric comparison and authentication of all U.S. visas and other travel and entry documents issued to aliens, and passports with biometric identifiers to be issued by Visa Waiver Program participating countries.[13]

The Intelligence Reform and Terrorism Prevention Act of 2004[14] required the collection of biometric exit data for all categories of individuals required to provide biometric entry data under US-VISIT,[15] regardless of the POE where they entered the United States. The law did not set a deadline for implementation of this requirement. The law also required DHS to develop a plan to accelerate the full implementation of the program.

[10] 8 U.S.C. § 1187(i).

[11] Pub. L. No. 107-173 (May 14, 2002).

[12] Pub. L. No. 108-299 (Aug. 9, 2004) extended the deadline from October 26, 2004, to October 26, 2005.

[13] Countries participating in the Visa Waiver Program are Andorra, Australia, Austria, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, The Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom.

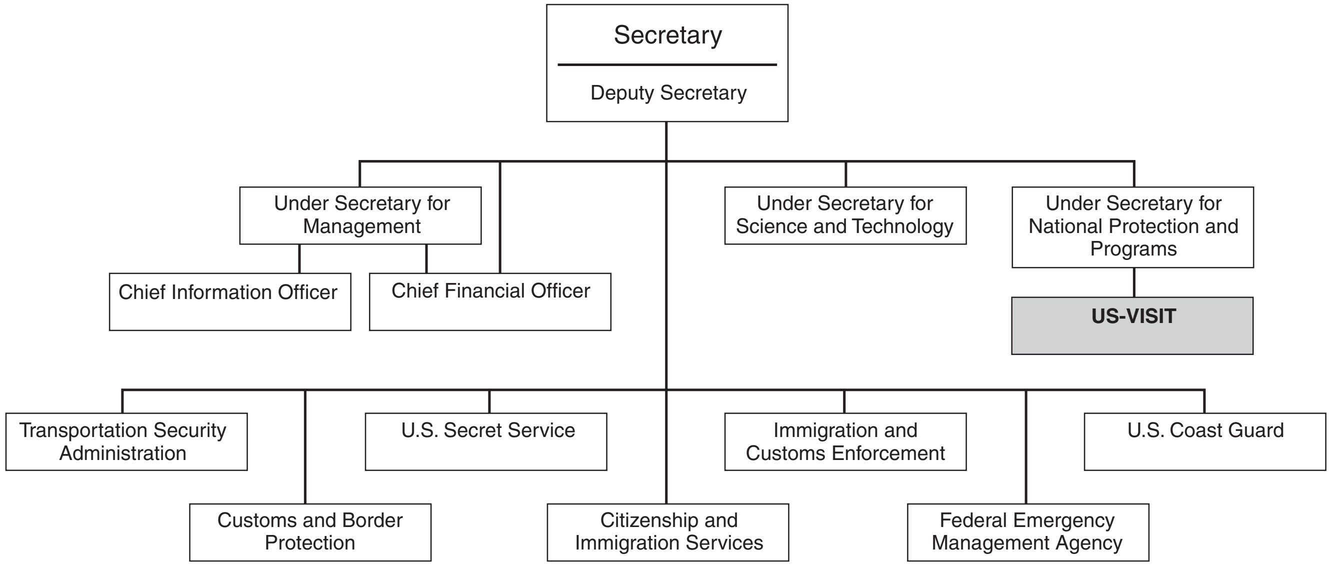
[14] Pub. L. No. 108-458, § 7208 (Dec. 17, 2004).

[15] US-VISIT currently applies to a certain group of foreign nationals—nonimmigrants from countries whose residents are required to obtain nonimmigrant visas before entering the United States and residents of certain countries who are exempt from U.S. visa requirements when they apply for admission to the United States for up to 90 days for tourism or business purposes under the Visa Waiver Program. US-VISIT also applies to (1) Mexican nonimmigrants traveling with a Border Crossing Card (BCC), who wish to remain in the United States longer than 30 days or who declare that they intend to travel more than 25 miles into the country from the border and (2) Canadians traveling to the United States for certain specialized reasons. See 8 C.F.R. § 235.1(f).

Overview of Program Structure and Organization

The US-VISIT program office is responsible for managing the acquisition, deployment, operation, and sustainment of US-VISIT. As of March 2007, the program office reports directly to the Under Secretary for National Protection and Programs. (See fig. 1.)

Figure 1: Simplified DHS Organizational Chart


Secretary
Deputy Secretary
Under Secretary for Management
Chief Information Officer
Chief Financial Officer
Under Secretary for Science and Technology
Under Secretary for National Protection and Programs
US-VISIT
Transportation Security Administration
U.S. Secret Service
Immigration and Customs Enforcement
U.S. Coast Guard
Customs and Border Protection
Citizenship and Immigration Services
Federal Emergency Management Agency

Source: GAO analysis of DHS data.

US-VISIT supports a series of homeland security-related mission processes that cover hundreds of millions of foreign national travelers who enter and leave the United States at about 300 air, sea, and land POEs. They are

- pre-entry, which is the process to evaluate a traveler's eligibility for required travel documents, enroll travelers in automated inspection programs, and prescreen travelers entering the United States;
- entry, which is the process of determining a traveler's admissibility to the United States at air, sea, or land POEs;
- status management, which is the process of managing and monitoring the changes and extensions of the visits of lawfully admitted nonimmigrant foreign nationals to ensure that they adhere to the terms of their admission and to notify appropriate government entities when they do not;

- exit, which is the process of collecting information on persons departing the United States; and
- analysis, which is the capability to provide for the continuous screening against watch lists of individuals enrolled in US-VISIT for appropriate reporting and action.

Overview of Program Status

DHS planned to deliver US-VISIT capabilities in a series of four increments: Increment 1 (air and sea entry), Increment 2 (air, sea, and land entry), Increment 3 (land entry), and Increment 4, which is to be a more strategic solution. Increments 1 through 3, which largely involved building interfaces among existing ("legacy") systems and enhancing the capabilities of these systems and supporting infrastructure, have been completed. As a result, a biometrically enabled entry capability is operating at about 300 POEs. More specifically, on January 5, 2004, the program office began operating most aspects of its planned biometric entry capability at 115 airports and 14 seaports for certain foreign nationals, including those from visa waiver countries.[16] As of December 2006, the program office was operating this entry capability in the secondary inspection areas of 154 of 170 land POEs.[17]

In September 2006, the program office deployed a capability to exchange limited information with IAFIS, which is the FBI's automated 10-fingerprint matching system. This capability, known as the interim Data Sharing Model (iDSM), was initially deployed September 3, 2006, and, according to the US-VISIT program office, is operating with the Boston Police Department, the Dallas County (TX) Sheriff, the Harris County (TX) Sheriff, and the Office of Personnel Management. Within the iDSM, IAFIS users have access to DHS biometrically-based information on expedited

[16] On September 30, 2004, US-VISIT expanded biometric entry procedures to include individuals from visa waiver countries applying for admission.

[17] According to program officials, 14 of the remaining 16 POEs have no operational need to deploy US-VISIT because visitors subject to US-VISIT are, by regulation, not authorized to enter into the United States at these locations. The other two POEs do not have the necessary transmission lines to operate US-VISIT, and thus they process visitors manually.

removals and Category 1 Visa Refusals.[18] Conversely, the Automated Biometric Identification System (IDENT) users have access to a limited set of IAFIS data that consists of active Wants and Warrants and Known/Suspected Terrorists.

The key systems that support or are connected to US-VISIT are described below. A simplified diagram of the relationships among these systems is shown in figure 2.

- IDENT collects and stores biometric data about foreign visitors, including information from the FBI, U.S. Immigration and Customs Enforcement (ICE) information on deported felons and sexual registrants, and DHS information on previous criminal histories and previous IDENT enrollments.
- IAFIS, which, as mentioned above, is the FBI's automated 10-fingerprint matching system and is electronically connected to all 50 states, as well as some federal agencies.
- Arrival Departure Information System (ADIS), which stores noncitizen traveler arrival and departure data received from air and sea carrier manifests and provides query and reporting functions. ADIS matches entry, immigration status updates, and departure data to provide immigration status, including whether the individual has overstayed his/her authorized period of stay.
- Student and Exchange Visitor Information System (SEVIS), which contains data on change of status throughout a foreign student's or exchange visitor's stay in the United States.
- Computer Linked Application Information Management System (CLAIMS 3), which includes adjudication results on foreign nationals who request immigration benefits such as change of status, extension of stay, or

[18] Under section 212 of the Immigration and Nationality Act (INA), as amended, an alien (nonimmigrant) is inadmissible if he/she does not have a valid passport, nonimmigrant visa, or border crossing identification card at the time of application for admission. 8 U.S.C. § 1182(a)(7)(B). Under the INA's expedited removal process, if an alien is inadmissible under section 212, the inspection officer may order the alien removed from the United States, without further hearing or review, unless the alien can demonstrate a credible fear of returning to his/her home country. 8 U.S.C. § 1225(b)(1)(A). Category 1 Visa Refusals include all the permanent ineligibilities for entry into the United States based on national security concerns, criminal activity, and the threat of spreading contagious disease.

adjustment to permanent resident status.

- Treasury Enforcement Communications Systems (TECS), which maintains lookout (i.e., watch list) data, interfaces with other agencies' databases, and is currently used by inspectors at POEs to verify traveler information and update traveler data.

- Advance Passenger Information System (APIS), which captures arrival and departure manifest information provided by air and sea carriers.

- Consular Consolidated Database (CCD), which is owned by the Department of State and includes information on visa applicants.

- Image Storage and Retrieval System (ISRS), which stores U.S. Citizenship and Immigration Services (USCIS) biometrics data, including the photo and fingerprints of individuals who have been issued a credential by USCIS.

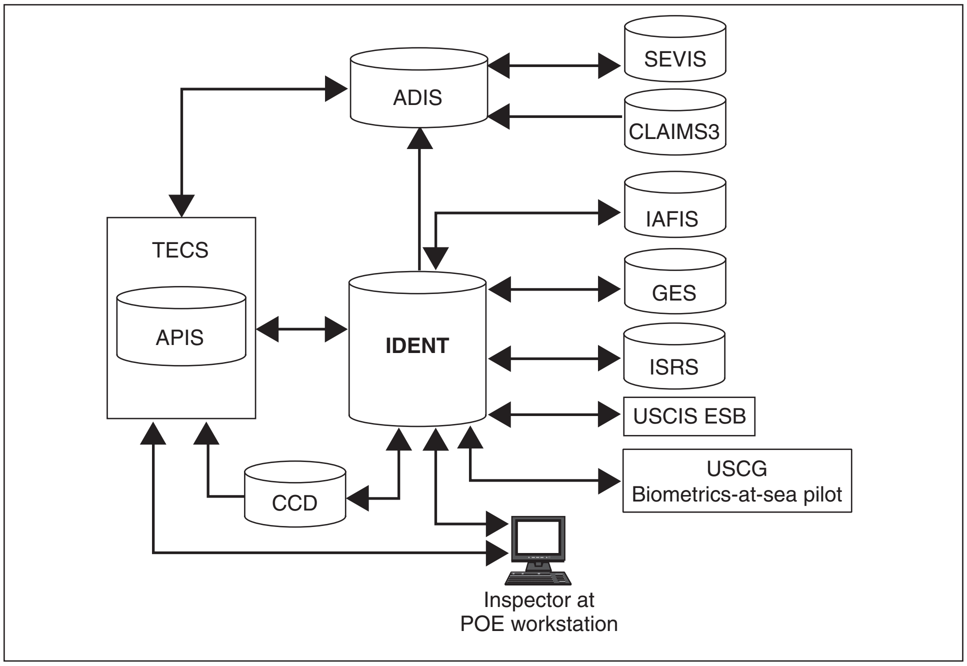
- The USCIS Enterprise Service Bus (ESB), which provides network connectivity in support of USCIS' "Inter-Country Adoption" program.

- The Global Enrollment System (GES), which supports the U.S. Customs and Border Protection (CBP) programs for expedited processing of preapproved, international, and low-risk travelers who voluntarily exchange information in return for expedited transit at U.S. borders.

- The U.S. Coast Guard's (USCG) Mona Pass Proof-of-Concept, which is to test the feasibility of deploying a mobile biometrics identification capability to a Coast Guard cutter in the Mona Passage.[19]

[19] The Mona Passage is located between the Dominican Republic and Puerto Rico. The objective of this effort is to demonstrate the feasibility of using biometric data (fingerprints) to identify and support prosecution of interdicted individuals. Interdicted individuals are enrolled in US-VISIT's IDENT database and are biometrically checked against known and suspected terrorists, aggravated felons, previous deportees, and recidivists.

Figure 2: Simplified Diagram of US-VISIT Related Systems



Source: GAO analysis of US-VISIT data.

Through fiscal year 2007, DHS had been appropriated about $1.7 billion and, as of October 2007, about $1.5 billion had been obligated for the US-VISIT program. For fiscal year 2008, the department has been appropriated $475 million for the program.

According to DHS, US-VISIT has produced mission value. For example, as of June 15, 2007, the program reported that it had more than 7,600 biometric hits in primary entry resulting in more than 1,500 people having adverse actions, such as denial of entry, taken against them. Further, about 14,000 leads were referred to the ICE immigration enforcement unit, resulting in 315 arrests.[20] Another potential consequence is the deterrent effect of having an operational entry capability. Although deterrence is difficult to demonstrate, officials have cited it as a byproduct of having a publicized capability at the border to screen entry on the basis of identity verification and matching against watch lists of known and suspected terrorists.

[20] We did not verify this information.

Overview of Biometric Technologies and Systems

Biometric technologies measure and analyze human physiological and behavioral characteristics. Identifying a person's physiological characteristics is based on direct measurement of a part of the body (e.g., fingertips, hands, face, eye retinas, and irises). Biometric measurements are theoretically effective personal identifiers because the characteristics measured (e.g., fingertips, hands, face, eye retinas, and irises) are thought to be distinct to each person. Therefore, unlike conventional identification methods that use something physical (e.g., an identification card), or a piece of information (e.g., a password), biometric identifiers are more reliable, cannot be forgotten, and are more difficult to lose, steal, or guess.

Biometric identification systems function as pattern recognition systems. They use acquisition devices, such as cameras and scanning devices, to capture images, recordings, or measurements of an individual's characteristics and computer hardware and software to extract, encode, store, and compare these characteristics.

Depending on the application, biometric systems can be used in one of two modes: identification or verification. Identification is referred to as one-to-many matching because an individual's presented biometric is compared against the stored biometric templates[21] of all individuals enrolled in the system. It is used to establish a person's identity—that is, to determine who a person is. Verification—also called authentication—is referred to as one-to-one matching because an individual's presented biometric is compared against the biometric for that person, which was stored in the system during enrollment. It is used to verify a person's identity—that is, to authenticate that individuals are who they say they are.

Other DHS Border Security and Immigration Initiatives

Besides US-VISIT, DHS has begun to plan and implement several other initiatives aimed at better securing our nation's borders and managing immigration matters, such as WHTI and SBI. WHTI was established pursuant to the Intelligence Reform and Terrorism Prevention Act of 2004, which required the Secretary of Homeland Security, in consultation with the Secretary of State, to develop and implement a plan that requires U.S. citizens and foreign nationals of Canada, Bermuda, and Mexico to present

[21] After a biometric system extracts the features of an individual's body part, it uses an algorithm to encode the features and store the information in a biometric template that can be used for future comparison.

a passport or other document or combination of documents deemed sufficient to show identity and citizenship to enter the United States.[22] As of January 23, 2007, citizens of the United States, Canada, Mexico, and Bermuda are required to present a passport to enter the United States when arriving by air from any part of the western hemisphere. This is currently not a requirement for these individuals when entering the United States via sea and land POEs from most countries within the western hemisphere.[23] On June 26, 2007, DHS and the Department of State issued a notice of proposed rulemaking for the implementation of WHTI at the sea and land environments. According to the proposed rule, DHS and the Department of State expect to implement WHTI by the summer of 2008.[24] We recently issued a report on the status of WHTI implementation to the House Homeland Security Committee's Subcommittee on Border, Maritime and Global Counterterrorism.[25]

SBI is a multiyear program that is to secure the borders and reduce illegal immigration by installing physical infrastructure and surveillance technologies along the border, increasing border security personnel, and ensuring information access to DHS personnel at and between POEs. A major component of SBI is called SBI*net*, which is to integrate personnel, infrastructures, technologies, and rapid response capabilities. DHS reports that SBI*net* is to encompass both the northern and southern land borders, including the Great Lakes, under a unified border control strategy whereby CBP is to focus on the interdiction of cross-border violations between and at the land POEs, funneling traffic to the land POEs. As part of SBI, DHS also plans to focus on interior enforcement—disrupting and dismantling cross-border crime into the interior of the United States while locating and

[22] Pub. L. No. 108-458, § 7209 (Dec. 17, 2004), as amended by Pub. L. No. 109-295, § 546 (Oct. 4, 2006) and Pub. L. No. 110–161, div. E, § 545 (Dec. 26, 2007).

[23] In November 2006, DHS and the Department of State issued a final rule announcing that, beginning on January 23, 2007, citizens of the United States, Canada, Mexico, and Bermuda are required to present a passport to enter the United States when arriving by air from any part of the western hemisphere. 71 *Fed. Reg.* 68,412 (Nov. 24, 2006). (To be codified at 8 C.F.R. Parts 212 and 235 and 22 C.F.R. Parts 41 and 53.)

[24] Since the date of the proposed rule, the Department of Homeland Security Appropriations Act, 2008, was enacted, which extended the WHTI implementation deadline. Pub. L. No. 110-161, div. E § 545 (Dec. 26, 2007). Specifically, the implementation shall not be earlier than the date that is the later of 3 months after the Secretaries of State and Homeland Security certify that certain criteria have been met, or June 1, 2009.

[25] GAO, *Observations on Implementing the Western Hemisphere Travel Initiative*, GAO-08-274R (Washington, D.C.: Dec. 20, 2007).

removing aliens who are in the United States illegally. We are currently conducting work for the House Homeland Security Committee to assess the development and deployment of SBI*net*'s command, control, and communications systems, and surveillance and detection systems. We are also reviewing DHS's use of performance-based services acquisition.

DHS's Enterprise Architecture Is Evolving and Is an Important Tool for Optimizing the Relationships among Related Programs

Effective use of an EA is a hallmark of successful private and public organizations. Generally speaking, an EA connects an organization's strategic plan with program and system solutions by providing the operational and technical information needed to guide and constrain implementable investments in a consistent, coordinated, and integrated fashion. This information consists of snapshots of both the enterprise's current ("As Is") environment and its target ("To Be") environment. These snapshots consist of "views," which are one or more interdependent and interrelated architecture products (e.g., models, diagrams, matrices, and text) that provide various representations of the enterprise. Managed properly, an EA can clarify and help optimize the interdependencies and relationships among an organization's business operations and the underlying information technology (IT) infrastructure and applications that support those operations. Moreover, when an EA is employed in concert with other important management controls, such as portfolio-based capital planning and investment control practices, it can greatly increase the chances that an organization's operational and IT environments will be configured to optimize mission performance. Our experience with federal agencies has shown that investing in IT without defining the investments in the context of an architecture often results in systems that are duplicative, not well integrated, and unnecessarily costly to maintain and interface.[26]

DHS issued the initial version of its EA in September 2003 and has continued to develop it since then, adding more scope and content to subsequent versions. In 2007, we reported on the third version of DHS's EA, stating that DHS had partially addressed shortcomings that we had identified in the previous versions. Since then, the department has further developed its architecture and issued an updated version. In doing so, it has continued to address our prior findings and recommendations.

[26] See, for example, GAO, *Homeland Security: Efforts Under Way to Develop Enterprise Architecture, but Much Work Remains*, GAO-04-777 (Washington, D.C.: Aug. 6, 2004); GAO, *DOD Business Systems Modernization: Limited Progress in Development of Business Enterprise Architecture and Oversight of Information Technology Investments*, GAO-04-731R (Washington, D.C.: May 17, 2004); GAO, *Information Technology: Architecture Needed to Guide NASA's Financial Management Modernization*, GAO-04-43 (Washington, D.C.: Nov. 21, 2003); GAO, *DOD Business Systems Modernization: Important Progress Made to Develop Business Enterprise Architecture, but Much Work Remains*, GAO-03-1018 (Washington, D.C.: Sept. 19, 2003); GAO, *Business Systems Modernization: Summary of GAO's Assessment of the Department of Defense's Initial Business Enterprise Architecture*, GAO-03-877R (Washington, D.C.: July 7, 2003); GAO, *Information Technology: DLA Should Strengthen Business Systems Modernization Architecture and Investment Activities*, GAO-01-631 (Washington, D.C.: June 29, 2001); and GAO, *Information Technology: INS Needs to Better Manage the Development of Its Enterprise Architecture*, GAO/AIMD-00-212 (Washington, D.C.: Aug. 1, 2000).

Prior GAO Reviews of US-VISIT Have Identified Several Areas for Improvement

Since 2003, we have issued numerous reports[27] highlighting fundamental challenges that DHS continues to face in defining the program. For example, we reported that DHS was investing in US-VISIT without a clearly defined operational context that included explicitly defined relationships among related border and immigration enforcement initiatives. In the absence of a DHS-wide operational context, program officials made assumptions about certain standard issues, such as capturing 2 fingerprints rather than 10 to identify foreign nationals subject to US-VISIT.

In December 2006,[28] we reported that DHS had launched key major border security programs, such as WHTI and SBI*net*, without adequately defining their relationships to US-VISIT. As a result, we concluded that DHS faces substantial risk that US-VISIT will not align with other immigration and border management initiatives and thus not cost effectively meet mission needs. We recommended that DHS determine how it expects to align emerging land border security initiatives, such as WHTI and SBI*net*, with US-VISIT, and what facility or facility modifications would be needed at land POEs to ensure that technology and processes work in harmony. In August 2007,[29] we reported that US-VISIT's strategic plan did not include any of the key elements associated with effective strategic plans. In particular, the plan did not explain the relationship between US-VISIT and other border management programs, such as WHTI, even though both programs involve the entry of certain foreign individuals at POEs.

[27] GAO, *Information Technology: Homeland Security Needs to Improve Entry Exit System Expenditure Planning*, GAO-03-563 (Washington, D.C.: June 9, 2003); GAO, *Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed*, GAO-03-1083 (Washington, D.C.: Sept. 19, 2003); GAO-04-586; GAO, *Homeland Security: Some Progress Made, but Many Challenges Remain on U.S. Visitor and Immigrant Status Indicator Technology Program*, GAO-05-202 (Washington, D.C.: Feb. 23, 2005); GAO, *Homeland Security: Recommendations to Improve Management of Key Border Security Program Need to Be Implemented*, GAO-06-296 (Washington, D.C.: Feb. 14, 2006); GAO, *Border Security: US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry*, GAO-07-248 (Washington, D.C.: Dec. 6, 2006); GAO, *Homeland Security: Planned Expenditures for U.S. Visitor and Immigrant Status Program Need to Be Adequately Defined and Justified*, GAO-07-278 (Washington, D.C.: Feb. 14, 2007); GAO, *Homeland Security: U.S. Visitor and Immigrant Status Program's Long–standing Lack of Strategic Direction and Management Controls Need to Be Addressed*, GAO-07-1065 (Washington, D.C.: Aug. 31, 2007).

[28] GAO-07-248.

[29] GAO-07-1065.

Over the last 5 years, we have also reported that DHS had not economically justified its investment in US-VISIT increments, including exit. For example, we reported in September 2003,[30] that DHS had not economically justified the initial increment (which was to include an exit capability at air and sea POEs) on the basis of benefits, costs, and risks. As a result, we recommended that DHS determine whether proposed incremental capabilities would produce mission value commensurate with program costs and risks. Similarly, in February 2006,[31] we reported that while DHS had analyzed the cost, benefits, and risks for its air and sea exit capability, the analyses did not demonstrate that the program was producing or would produce mission value commensurate with expected costs and benefits, and the costs upon which the analyses were based were not reliable. A year later, we reported[32] that DHS had not adequately defined and justified its past investment in its air and sea exit pilots and its land exit demonstration projects. We recommended, among other things, that planned expenditures be limited for exit pilots and demonstration projects until such investments were economically justified.

US-VISIT Strategic Solution Is Not Fully Defined, and No Aspects Were Economically Justified Prior to Solution Development

Thus far, DHS has partially defined a US-VISIT strategic solution. On the basis of available project documentation, we determined that the strategic solution consists of two primary components: (1) Unique Identity and (2) exit. Of these, the first is fairly well-defined, the second is not. Further, although Unique Identity is defined, it was not economically justified in a timely fashion, and thus DHS proceeded with its development in the absence of an analytically verifiable basis for doing so. The absence of a fully defined strategic solution and timely economic justification hinders informed decision making about the best course of action for accomplishing strategic program goals and inhibits the ability to measure performance and promote accountability.

[30] GAO-03-1083.

[31] GAO-06-296.

[32] GAO-07-278.

The Unique Identity Component of US-VISIT Strategic Solution Has Been Defined and Is Under Development

One of the two major components of the strategic solution is a project known as Unique Identity. The purpose of this project is to develop and deploy a capability that establishes a single identity for all individuals encountered across the immigration and border mission area. This is to be achieved by capturing the individual's biometrics, including 10 fingerprints and a digital image, at the earliest possible interaction with any immigration and border management entity (e.g., when the individual is applying for a visa or immigration benefit). It is also to enable an improved process for determining the risk associated with allowing entry to an individual or the individual's eligibility to receive benefits.

Unique Identity consists of the development of three capabilities: (1) 10-print identification, (2) enumeration, and (3) IDENT/IAFIS interoperability. These capabilities are to be fully deployed by 2010 and as of November 7, 2007, the program office reported obligating about $65 million, and expending about $22 million,[33] to develop and deploy Unique Identity.

Ten-print Identification

Ten-print identification is to establish the means for capturing 10 fingerprints and is to enable the other two Unique Identity components, as well as increase the fingerprint matching accuracy in IDENT.

The first three increments of US-VISIT were deployed using 2-print identification and verification capability. In July 2005, DHS announced that it intended to biometrically screen foreign visitors to the United States based on a fingerprint standard of 10-print flat capture at enrollment and fewer than 10 fingerprints for verification thereafter. This work was required for POEs and the Department of State posts that were participating in the Biometric Visa (BioVisa) program,[34] both of which were collecting 2 fingerprints. Transitioning to 10 fingerprints also required modifications to IDENT to accept and process the larger number of fingerprints.

[33] Since 2006, we have reported that the system that US-VISIT uses to manage its finances, ICE's Federal Management System has reliability issues. Although many issues are no longer considered material weaknesses, independent auditors are still unable to express an opinion on DHS's balance sheets as of September 30, 2007.

[34] Section 303 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Pub. L. No. 107-173) requires that no later than October 26, 2004, the Department of State issue visas that use biometric identifiers. Pub. L. No. 108-299 (Aug. 9, 2004) extended the deadline from October 26, 2004 to October 26, 2005.

US-VISIT and other agencies that either had a need or developed guidance for biometrics (e.g., the FBI, Department of State, and the National Institute of Standards and Technology [NIST]) established a user group and began working with industry to determine whether there were 10-print scanners available that met their respective requirements, such as maximum size and processing speed. In December 2005, the user group determined that the 10-print scanners available at that time did not meet these requirements, but that such scanners could be available within 12 months. In November 2006, the Department of State, which was able to employ the already available scanners, began to capture 10 fingerprints, as a pilot, during visa issuance in overseas embassies and consulates. According to the US-VISIT program office, the Department of State has deployed 10-print equipment to all of its visa-issuing posts.

By January 2007, technology improved to the point where US-VISIT was able to evaluate vendor proposals for 10-print scanners. That same month, the program office awarded contracts to two scanner vendors that had developed technically suitable devices. Currently, the program office is deploying 10-print scanners on a pilot basis to 10 air locations[35] that currently use a 2-print scanner and, according to a US-VISIT official, it plans to complete this deployment and begin evaluating the scanners' performance in March 2008. Full deployment to all locations that currently use a 2-print scanner (including primary inspection lanes in air and sea POEs and secondary inspection lanes in land POEs) is scheduled to be completed by December 2008.

Enumeration

Enumeration is to associate the biometric and biographical data within IDENT and IAFIS with individuals encountered by immigration and border management entities and thereby allow for improved risk and eligibility determinations for individuals entering the United States or applying to receive benefits. When decisions are made concerning entry or eligibility, details from these encounters are also to be recorded and linked to the individual's record. To accomplish this, a unique identifier, referred to as

[35] The 10 planned locations are Washington Dulles International Airport (Chantilly, VA), John F. Kennedy International Airport (New York, NY), Detroit Metropolitan Wayne County Airport (Detroit, MI), William B. Hartsfield International Airport (Atlanta, GA), Chicago O'Hare International Airport (Chicago, IL), General Edward Lawrence Logan International Airport (Boston, MA), Orlando International Airport (Orlando, FL), San Francisco International Airport (San Francisco, CA), Miami International Airport (Miami, FL), and Houston International Airport (Houston, TX).

an enumerator,[36] is assigned to the individual's record, stored within IDENT, and linked to the fingerprints and the individual's associated biographic information. Upon subsequent interactions, the individual's identity is to be biometrically verified and information about the individual, including past encounters, is to be available for risk and eligibility decisions.

Enumeration begins with the person's initial encounter by immigration and border management entities. During this encounter, an individual's biometrics (i.e., 10 fingerprints and digital image) and limited biographical information are captured. Once this information is gathered, one of three enumeration services can be provided: identify, verify, or retrieve encounter details. These services are described here.

- *Identify*: IDENT is searched using the biometrics captured from the individual during the initial encounter to determine whether biometric records are stored in the system. The individual's fingerprints are enrolled in IDENT and if no matching biometric record is found, an enumerator is assigned. If a biometric record is already stored in IDENT, but without an enumerator, one is assigned. IAFIS is then searched using the collected biometrics.

- *Verify*: If a person has already been enumerated, IDENT and IAFIS are searched and the individual's identity is verified against the stored biometric records.

- *Retrieve Encounter Details*: A request can be submitted for details of a particular previous encounter with the individual. Using the enumerator, biometric and related biographic information for the individual is retrieved and provided to aid the risk or eligibility decision.

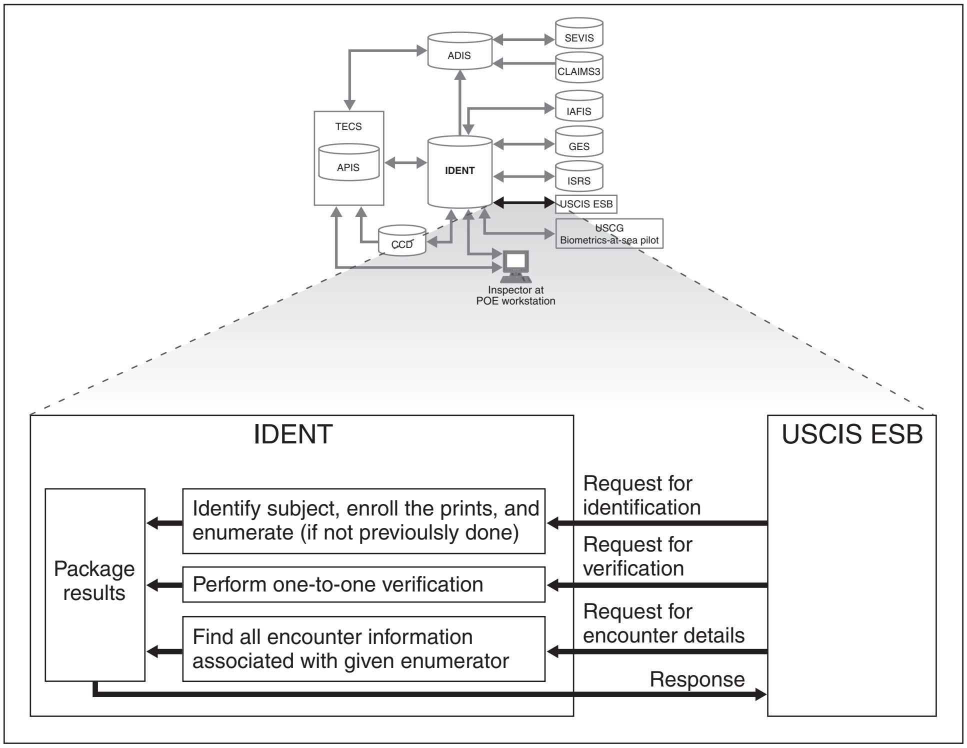
The results of these requests are packaged and returned by IDENT, and may include a list, and types, of the individual's previous encounters.

Thus far, enumeration services have been implemented on a pilot basis. Specifically, in July 2007, USCIS implemented enumeration services as part of its Inter-Country Adoption process, which is to allow USCIS

[36] The enumerator is an alphanumerical identifier that is to link disparate records pertaining to an individual, such that these records can be linked and accurately retrieved, regardless of location, platform or issuing entity. It can be used for identification purposes within DHS and by other immigration and border management organizations.

adjudicators and other users to store, retrieve, and update centrally stored information about inter-country adoption cases. A simplified diagram of the enumeration process, as utilized by USCIS, and the types of enumeration requests, can be found in figure 3.

Figure 3: Simplified Diagram of Enumeration as Used by USCIS


ADIS
SEVIS
CLAIMS3
TECS
APIS
IDENT
IAFIS
GES
ISRS
USCIS ESB
USCG
Biometrics-at-sea pilot
CCD
Inspector at
POE workstation
IDENT
USCIS ESB
Package results
Identify subject, enroll the prints, and enumerate (if not previoulsly done)
Perform one-to-one verification
Find all encounter information associated with given enumerator
Request for identification
Request for verification
Request for encounter details
Response

Source: GAO analysis of US-VISIT data.

USCIS' Inter-Country Adoption Pilot is part of the USCIS transformation program, which is to transition USCIS from a form-based to a "person-centric," or customer account-based, service provider. Successful transition depends on the capability to uniquely identify and validate a person's identity in order to track and manage the ongoing relationship of the person with USCIS. According to the USCIS Chief Information Officer, USCIS plans to eventually associate all of its immigration and border management records with the enumerator.[37]

However, future implementation of enumeration by other DHS organizations is uncertain. The US-VISIT Program Director told us that the use of enumeration has not been mandated across the department. He added that departmentwide use of the capability could be 5 years away, but that they are deploying the service to meet USCIS's requirement. Because of this, program officials stated that a deployment plan for departmentwide use of enumeration does not exist. Instead, they intend to provide the capability to DHS entities on an as requested basis.

IDENT/IAFIS Interoperability

The purpose of IDENT/IAFIS interoperability is to enable DHS and the FBI to share biometric and related biographic, criminal history, and immigration history data. To achieve this interoperability, the program office is working with the FBI's Criminal Justice Information Services Division, which manages IAFIS. DHS and the FBI plan to deploy IDENT/IAFIS interoperability in three phases, each of which is to build on the previous phase and to provide increased information sharing. The three phases are iDSM, Initial Operating Capability (IOC), and Full Operating Capability.

- *The interim Data Sharing Model* is a proof-of-concept for long-term information sharing between DHS and the FBI. Under iDSM, as mentioned previously, DHS provides the FBI with information on expedited removals and Category 1 Visa Refusals, and the FBI provides DHS with information on active Wants and Warrants and Known/Suspected Terrorists. These data are shared by providing and storing copies of the data (e.g., Visa Refusals and Wants and Warrants, respectively) in repositories that are outside of the IDENT and IAFIS systems but that are located at the other agency's data center. Ownership and control of the agencies' data subsets are still maintained by the originating agency.

To illustrate, copies of DHS fingerprint images and limited biographic information, such as name and date/place of birth, are transmitted from IDENT to the separate IDENT repository located in the DOJ data center.

[37] Although US-VISIT plans to have enumeration search and link to information found in IAFIS, the USCIS Chief Information Officer stated that, initially, USCIS will not search IAFIS information when making a request because of fees charged by the FBI for accessing IAFIS, noting that USCIS already had an interface to IAFIS. According to the same official, USCIS plans to make use of IDENT/IAFIS interoperability once it is deployed.

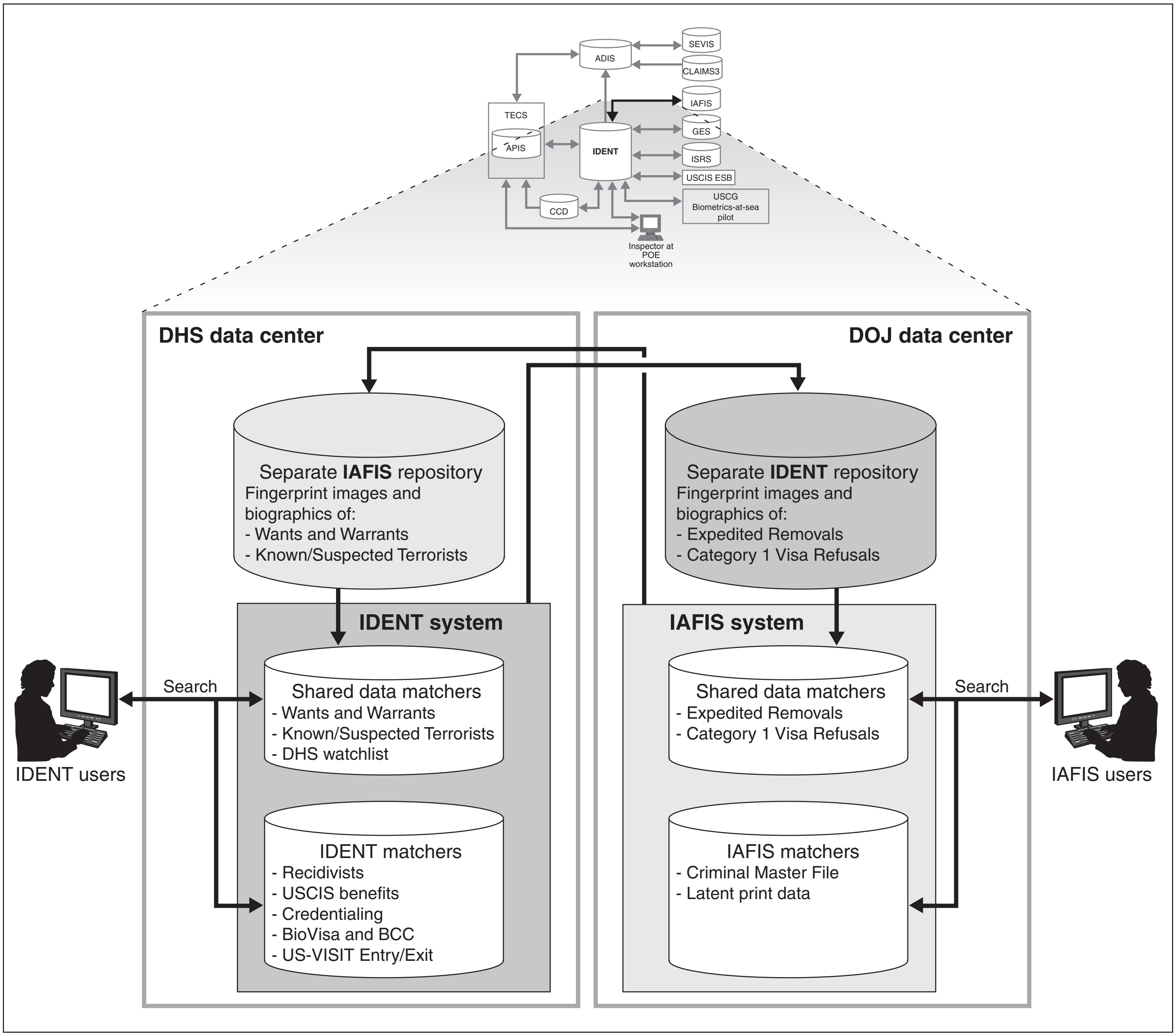
Once the information has been placed within the repository, it is then sent to the DOJ/IAFIS shared data fingerprint matchers,[38] which reside within the IAFIS system. Once the information is in the matchers, minutiae are extracted from the fingerprint images and stored in the matchers along with the limited biographic information. DOJ/FBI shares the IAFIS data with DHS in the same way.

When users submit a query, both the shared data matchers (which contain the copies of the other agency's data) and their own data matchers are searched for potential hits. For example, when an IDENT user submits a query, both the IDENT shared data matchers that contain copies of the FBI's Wants and Warrants and the Known/Suspected Terrorists data, and the IDENT matchers that contain DHS's biometric and biographical data are searched for biometric matches. (See fig. 4 for a simplified diagram of the iDSM architecture.)

The iDSM was deployed September 3, 2006, and, according to the US-VISIT program office, is operating with the Boston Police Department, the Dallas County (TX) Sheriff, the Harris County (TX) Sheriff, and the Office of Personnel Management.

[38] A fingerprint matcher is an automated identification system that searches against databases that store minutiae information for fingerprint images. A minutiae point is a break in a fingertip ridge in a fingerprint image. A typical fingerprint image may produce between 15 and 50 minutiae, depending on the portion of the image captured. These minutiae are used in matching with other fingerprints.

Figure 4: Simplified Diagram of iDSM Architecture

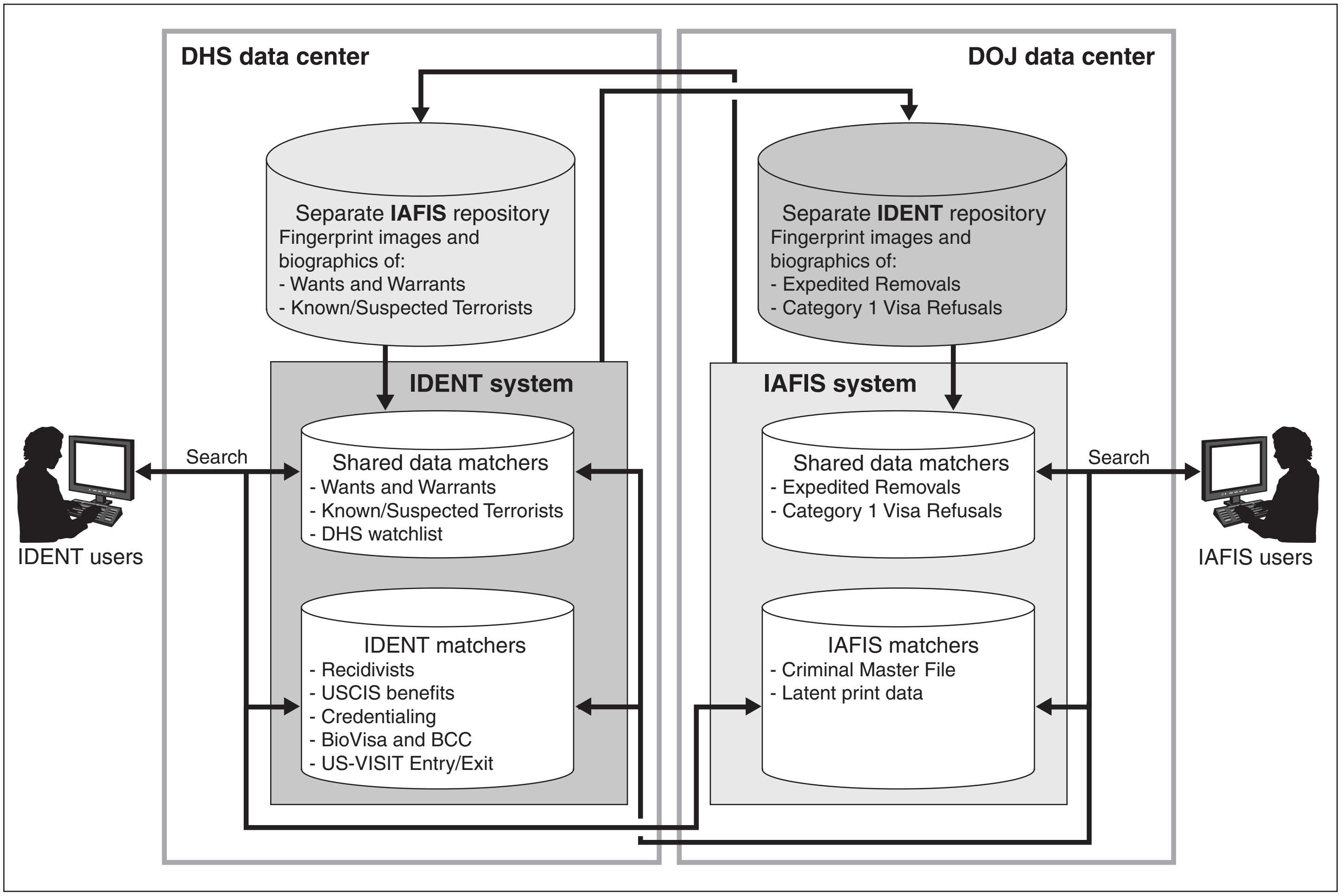


Source: GAO analysis of US-VISIT data.

- *Initial Operating Capability* is to expand the data sets to be shared between IDENT and IAFIS. In addition to the data shared as part of iDSM, DHS is to also share its entire recidivist repository, USCIS benefits data, credentialing information, additional information from the BioVisa and BCC programs, DHS watchlist data, and enrollment/enumeration and encounter data. In turn, the FBI is to share 55 million records in the Criminal Master File, as well as latent print data.

In addition, IOC is to modify the architecture for sharing the expanded set of IDENT and IAFIS data. Under IOC, the data shared between IDENT and IAFIS as part of iDSM will continue to be shared as it is under the iDSM architecture (i.e., copies of the shared data are sent to separate repositories and data matchers). In addition, DHS and the FBI are to share the additional data sets (e.g., recidivist repository and Criminal Master File, respectively) by providing direct access to the actual fingerprint data (as opposed to copies in the iDSM architecture) stored in each other's fingerprint matchers. Similar to iDSM, all respective matchers are to be searched as part of a single query. To illustrate, when an IDENT user submits a biometric search query, three matchers are searched: (1) the IDENT shared data matchers that contain copies of the FBI's Wants and Warrants and the Known/Suspected Terrorists data, (2) the IDENT matchers that contain DHS's biometric data, and (3) the IAFIS matchers that contain the Criminal Master File and latent print data. Similar data matchers are searched for an IAFIS user query, except that the IDENT shared database is also searched because it includes DHS watchlist data, in addition to the IAFIS shared data. According to the US-VISIT Program Director, IOC is planned for September 2008. (See fig. 5 for a simplified diagram of the proposed IOC architecture.)

Figure 5: Simplified Diagram of IOC Architecture



Source: GAO analysis of US-VISIT data.

- *Full Operating Capability* refers to the end state of interoperability between IDENT and IAFIS. It is to provide for interoperability and real-time data sharing of an expanded set of biographic data for criminal and civil searches. However, the exact information to be shared by DHS and the FBI has not yet been determined. Full Operating Capability is planned for February 2010.

The Exit Component of US-VISIT Strategic Solution Has Not Been Adequately Defined

Despite long-standing legislative requirements and a sizeable investment of time and resources, DHS has yet to clearly define the second major component of its strategic solution—exit. Moreover, while DHS has established milestones for several key air exit activities, such as fully implementing an air exit capability by the end of 2008, the program office has not provided any verifiable analysis and documentation that support these milestones, thus calling into question their reliability. According to DHS officials, the current state of exit capabilities owes largely to the fact that an exit capability is more challenging to implement than entry. Without an operationally effective exit capability, US-VISIT cannot meet its strategic goals, and the integrity of the nation's immigration system is limited. Further, the absence of any defined exit solution, including reliable milestones, means that this situation is not likely to change in the near future.

As mentioned earlier, the legislative underpinnings for an exit capability were established in 1996.[39] In response, DHS allocated about $260 million for exit-related efforts between 2003 and 2007, and the program office reports that it expended about $157 million. In particular, the program office conducted various exit pilots and demonstration projects at air, sea, and land POEs. Throughout this period, we reported on the limitations in how these activities were planned, defined, and justified. Most recently, we reported in August 2007[40] that the lack of a well-defined and justified exit solution risks repeating failed and costly past exit efforts. We further reported that no exit program plans were available that defined what will be done, by what entities, and at what cost to define, acquire, deliver, deploy, and operate this capability, including plans describing expected system capabilities, defining measurable outcomes (benefits and results), identifying key stakeholder (e.g., airlines) roles/responsibilities and buy-in, and coordinating and aligning with related programs.

DHS has recently reaffirmed its commitment to implementing an exit solution and reconstituted its efforts. In particular, DHS reports that it will

[39] Specifically, the IIRIRA required the development of an automated system to record and then match the departure of every foreign national from the United States to the individual's arrival record. Subsequently, the Immigration and Naturalization Service Data Management Improvement Act of 2000 amended the IIRIRA and required an electronic system to record the entry and exit of certain foreign nationals, and the Intelligence Reform and Terrorism Prevention Act of 2004 specifically required that US-VISIT include the collection of biometric exit data for all individuals for which entry data was available.

[40] GAO-07-1065.

focus first on a biometric air exit solution by leveraging existing commercial airlines processes. However, the means by which this integration is to be accomplished has yet to be defined and published. Currently, DHS plans to issue a Notice of Proposed Rule Making for establishing a biometric exit verification process at commercial international air exit points.

To date, we have yet to receive further details on the proposed process beyond a high-level schedule of key milestones, which includes issuing the proposed and final rules by December 2007 and June 2008, respectively, and fully implementing the air exit solution by December 2008. However, these milestones are not supported by the kind of verifiable analysis and documentation that is associated with reliably derived program schedules, such as (1) decomposition of the program into a work breakdown structure; (2) sequencing, integration, and resourcing of each work element in the work breakdown structure; and (3) identification of the critical path through the schedule of linked work elements. As a result, the reliability of the milestones remains questionable. Further, the milestones are dependent on several major unknowns. For example, until the proposed rule is issued and comments are received, DHS will not know the full scope and nature of any airline concerns and challenges, which may affect the content of the final rule; this final rule will in turn dictate what the airlines will be required to do and thus what their respective time lines will be for implementing their parts of the exit solution. Exacerbating this lack of reliability with the reported air exit milestones is the fact that the program office has already missed several near-term milestones. For example, it was to complete an alternatives analysis, the business requirements, and a concept of operations by August 2007, as planned. As of November 2007, the program office reported that these documents had yet to be approved. Further, it did not meet the December 2007 date for issuing the proposed rule.[41]

With regard to sea and land exit, a strategic solution is even less defined and thus more uncertain. While DHS reports that it will develop and deploy a sea exit capability that emulates its air exit solution, no plans are available that define what entities are to be involved, how much the solution will cost, or when it will be deployed. For land, DHS has not determined a time frame or cost estimates for even initiating a land exit

[41] In its technical comments on a draft of this report, DHS stated that it had developed a project management plan.

solution. In lieu of deploying this capability, DHS plans to initially explore options for expanding the collection of biographic data on travelers crossing the borders. Specifically, the then-acting US-VISIT Director of Program Integration and Mission Services told us that US-VISIT is building relationships with Canada to foster future possibilities of sharing border operation information. Further, while the Comprehensive Exit Charter notes that, as biometric scanning technology develops and becomes more sophisticated, DHS will consider land exit options that provide for biometric capture without severely impacting the flow of travel across the border, but no further details are available.

The longer the department goes without an exit capability, the more its ability to effectively and efficiently perform its border security and immigration enforcement missions may suffer. Without exit data, for example, DHS cannot ensure the integrity of the immigration system by identifying and removing those people who have overstayed their original period of admission—a stated goal of US-VISIT.

DHS Did Not Economically Justify Investing in Unique Identity in a Timely Fashion

The decision to invest in any system should be based on reliable analyses of estimated system costs and expected benefits over the life of the investment. Given the importance of these analyses to informing the decision-making process, they should be completed prior to selecting and investing in a particular solution to ensure that the solution selected achieves the expected performance goals with the lowest life cycle costs and the least risk. This is consistent with Office of Management and Budget guidance, which states that individual increments of major systems are to be individually supported by analyses of benefits, cost, and risk.[42] DHS has also issued guidance recognizing the importance of completing such economic analyses early in a project's planning stage to support informed decision making about what projects should be approved and funded.[43]

While DHS developed a cost-benefit analysis for Unique Identity, the analysis was completed after system development activities were well under way. Specifically, DHS completed an analysis for Unique Identity in

[42] Office of Management and Budget, *Planning, Budgeting, Acquisition and Management of Capital Assets*, Circular A-11, Part 7 (Washington, D.C.: June 21, 2005).

[43] Department of Homeland Security, *Capital Planning and Investment Control: Cost-Benefit Analysis (CBA) Guidebook* (February 2006).

August 2006, but the analysis did not address the alternative solution that DHS ultimately selected and is now being developed. Subsequent to the completion of the August 2006 analysis, the program office and the FBI elected to pursue a hybrid alternative solution that was not included in the initial analysis, in part to address the FBI's interest in maintaining control over FBI data to be shared with IDENT. According to program officials, when the hybrid solution was developed, they considered the degree of technology change required for the hybrid and, based on the potential changes, determined that any increased cost would be marginal. However, they could not provide any documented evidence to support this determination.

Subsequently, in October 2007, DHS issued a revised analysis that included the alternative solution that is being pursued. However, this analysis was about 14 months after the initial phase of Unique Identity was deployed and after about $65 million was obligated, and $22 million was expended. According to program officials, the revised analysis confirmed that its costs and benefits were roughly equivalent to the original analysis and affirmed the program's decision to select and build this alternative. However, program officials agreed that given that the solution has been selected and is being developed, the value of such an "after-the-fact" analysis in informing investment decision making is lost. By following such a practice, DHS did not know whether it was pursuing the most cost effective investment option until after it had obligated tens of millions of dollars.

In addition, DHS has yet to finalize a cost-benefit analysis for a comprehensive exit solution. According to program officials, the department intends to finalize such an analysis for its air exit solution as part of the Notice of Proposed Rule Making process. However, it is unclear if and when an analysis will be completed for the sea and land solutions.

DHS Continues to Focus on Fingerprints as Its Primary Biometric Technology

DHS considered various biometric technologies, including fingerprints, facial, and iris technologies, and continues to use fingerprints as its foundational biometric. According to NIST and DHS, fingerprint technology is currently the most accurate form of biometric identification for matching one biometric record against many such records, which is a key requirement of US-VISIT. Notwithstanding this focus on fingerprints, the program office continues to participate in and review research efforts examining other forms of biometrics and how those technologies might be applied to US-VISIT. In recognition that one of these technologies may prove viable, the program office modified IDENT to allow an additional mode of biometric comparison if such technology becomes feasible.

DHS Considered Various Biometric Technologies, Focusing on Fingerprints as Its Foundational Biometric

While DHS has considered various biometric technologies, including fingerprints, facial, and iris technologies, it maintains its focus on fingerprints as its foundational biometric technology for two primary reasons. First, fingerprint technology is currently the most accurate form of biometric identification for matching one biometric record against many. According to the Chief of NIST's Information Access Division, who is responsible for overseeing biometric technology research, no biometric technology, other than fingerprints, has been demonstrated operationally, or in independent testing, to automatically and accurately identify one-to-many matching on US-VISIT sized populations. Such matching is performed by IDENT, which contains fingerprints collected from a number of sources.[44] Second, focusing on fingerprint technology provides DHS with access to the FBI's biometric database, known as IAFIS.

However, IDENT's use of a 2-print model—one from the left index finger and one from the right index finger—has been identified as a major barrier for achieving interoperability with IAFIS, which is a 10-print system. Interoperability between IDENT and IAFIS provides DHS and US-VISIT access to the largest criminal biometric database in the world, the Criminal Master File, which, as mentioned previously, stores over 50 million sets of 10 rolled fingerprints and corresponding criminal history information submitted by law enforcement agencies. IAFIS also contains a Civil Subject Index Master File, which stores noncriminal fingerprints (e.g., fingerprints of military, government, or authorized nongovernment personnel), and an Unsolved Latent File, which contains latent fingerprint[45] images found at crime scenes. In May 2007, DHS designated IDENT as the DHS biometric repository and committed to moving it to 10 fingerprints in order to enhance US-VISIT's ability to identify and verify a person's identity. According to NIST officials, this is because a system's accuracy increases as a greater number of fingerprints are used.

[44] Includes data such as: FBI information on all known and suspected terrorists, selected wanted persons (foreign-born, unknown place of birth, previously arrested by DHS), and previous criminal histories for high-risk countries; DHS ICE information on deported felons and registered sex offenders; and DHS information on previous criminal histories and previous IDENT enrollments.

[45] A latent print is fingerprint "image" left on a surface that was touched by an individual. The transferred impression is left by the surface contact with the friction ridges, usually caused by the oily residues produced by the sweat glands in the finger.

The environment in which US-VISIT operates limits the effectiveness of other biometric technology options. A program official who works with biometrics told us that one of the limitations of capturing high-quality photographs for facial recognition is that the POE environment cannot be modified to, for example, change the background in the photos of individuals. Specifically, a backdrop for taking photos cannot be placed in a POE because it will restrict the CBP officers' view of the processing area.

Other Biometric Technologies Remain a Future Option

Although DHS is using fingerprints as its primary biometric identifier, it has ongoing biometric research efforts. For example, the program office works with academic institutions, such as the Center for Identification Technology Research at West Virginia University, to explore the rapidly growing area of biometric identification technology. Further, the program office has contracted with NIST to conduct research and analysis on biometric capture devices, systems, and procedures in a range of operational environments. In addition, a program office representative chairs the DHS Biometrics Coordination Group, which facilitates DHS intradepartmental planning and coordination for biometrics research, development, testing, and evaluation. As part of this, the Research and Development, Testing and Evaluation Working Group within the Biometrics Coordination Group gathers research and development requirements and shares them with other groups, such as the Human Factors Division within the DHS Science and Technology Directorate and the National Science and Technology Council Subcommittee on Biometrics and Identity Management.

In addition, program officials stated that US-VISIT is beginning to evaluate how to add the capability to process multiple types of biometrics—also known as multimodal biometrics—in the next 3-5 years. Further, program officials stated that IDENT has been modified to add the capacity and capability to eventually receive and match biometric data from technologies other than fingerprints, should another type of biometric mature to where it can be effectively used. Program officials also stated that US-VISIT plans to conduct prototype work on multimodal biometric data in order to increase the accuracy and efficiency of matches. Additional details about biometric technologies are in appendix III.

Efforts to Define, Manage, and Coordinate Relationships among US-VISIT and Other Border Security Programs Are Evolving

Because optimizing an organization's ability to achieve its strategic goals and outcomes depends in part on its success in managing the interdependencies among related programs, it is essential that DHS define, manage, and coordinate its border screening programs in a way that embodies collaboration practices that our research shows are important to maximizing organizational performance and achieving organizational goals and outcomes. While DHS has established a few mechanisms for defining and managing related immigration and border programs, including US-VISIT, WHTI, and SBI*net*, and begun to implement key collaboration practices, these activities are still evolving. Going forward, it is important that DHS embrace and maximize the use of key organizational collaboration practices to effectively manage the relationships among these programs. Absent such collaboration, DHS risks potential overlap, duplication, and inconsistency across the programs, which could limit effective and efficient organizational performance and results.

As we have previously reported,[46] organizational collaboration can be viewed as any joint activity that is aimed at producing more public value than could be produced when programs or organizations act alone. Among other things, our research shows that effective collaboration depends on the use of certain collaboration practices. These practices include

- *establishing common outcomes*: defining and articulating a shared or common outcome(s) or purpose(s) that organizations or programs are mutually seeking to achieve and that are consistent with their respective goals and missions;

- *establishing mutually reinforcing or joint strategies*: creating strategies that work in concert with those of their partner organizations or programs, or that are joint in nature;

- *leveraging resources*: identifying the human, technological, physical, and financial resources needed to initiate or sustain the collaborative effort;

- *agreeing on roles and responsibilities*: working together to define and agree on respective roles and responsibilities, including how the collaboration efforts will be led;

[46] GAO, *Results–Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: Oct. 21, 2005).

- *establishing a compatible means to operate across organizational boundaries*: creating compatible standards, policies, procedures, and data systems that will be used in the collaborative effort; and
- *developing mechanisms to monitor, evaluate, and report on results*: putting in place the means to monitor, evaluate, and report on the collaborative effort to identify areas for improvement.

Most of these practices are reflected to some degree in department-level mechanisms that are in place and are evolving, such as the DHS EA and the Screening Coordination Office (SCO). Similarly, limited program-to-program collaboration efforts are occurring. As these efforts continue to evolve, it is important to examine the expanded use of these collaboration practices. DHS's implementation of each of the practices, along with opportunities for their expanded use, is discussed below.

Establishing a Common Outcome

DHS's strategic plan and EA (the department's blueprint for implementing its strategic plan), define outcomes for securing our nation's border that are shared by US-VISIT, WHTI, and SBI*net*. In particular, one of the goals in the department's strategic plan is to detect, deter, and mitigate threats to our homeland, and one of its objectives for achieving this goal is to secure our borders against terrorists, the means of terrorism, illegal drugs, and other illegal activity. US-VISIT, WHTI, and SBI*net* program documentation explicitly link their programs to this common goal and objective. For example, one of US-VISIT's goals is to enhance the security of U.S. citizens and visitors and one way it seeks to achieve this is by matching foreign nationals' biometrics against watch lists, thereby preventing those visitors who may pose a threat from entering the country.

In addition, the EA's draft transition plan groups programs, including US-VISIT and WHTI, that have a common purpose (namely, assessing the risk and determining the eligibility of persons seeking to enter the United States, or obtain a benefit or credential)[47] into a portfolio of screening programs.[48] According to the DHS Chief Architect, SBI*net* will be included in the screening/watchlist portfolio and reflected in the department's next EA transition plan.

[47] A credential is a certified document showing that a person has a certain privilege, right, or status.

[48] Portfolios are groupings of related investments, projects, systems, and services.

Notwithstanding DHS's efforts to link the three programs to common strategic outcomes, other shared aspects of the programs are not as well-established. For example, the EA does not define how these programs are expected to share common services and data. Specifically, it does not yet include an inventory of services to be provided by each program such as the biometric services that US-VISIT provides in support of the department. Similarly, it does not include a complete inventory of DHS data assets relevant to the screening programs.[49] For example, while it identifies and describes 20 data assets, including IDENT and ADIS, the EA does not include all of the biographic data assets that support identity management and screening processes, such as SEVIS, which ICE uses to manage and monitor the stay of foreign students in the United States.

Moreover, program-to-program level activities aimed at identifying and pursuing common strategic outcomes are not apparent. Specifically, while US-VISIT program officials told us that potential relationships with other immigration and border management programs, including WHTI and SBI*net*, exist, they have not yet been defined. With regard to WHTI in particular, a program official said that the program office intends to work with the WHTI program office to implement radio-frequency identification (RFID) technology[50] for US-VISIT land exit, but efforts for accomplishing this have yet to go beyond providing the WHTI program office with the results of US-VISIT's land exit RFID "proof-of-concept" pilot projects, as well as the associated hardware.[51] Similarly for SBI*net*, while the business needs assessment for US-VISIT's mobile biometric link project[52] identifies SBI*net* as a potential user of this capability, the assessment states that SBI*net* is to develop a solution to enable border patrol agents to process biographic and biometric information in remote border areas. According to US-VISIT officials, the US-VISIT/SBI*net* relationships have not yet been defined.

[49] A data asset is a managed container for data such as a database, Web site, document repository, or directory.

[50] RFID technology can be used to electronically identify and gather information contained on a tag.

[51] US-VISIT utilized RFID technology embedded in a tag on a visitor's arrival/departure form—which an electronic reader at the POE was intended to detect. For the implementation of WHTI in the land environment, DHS anticipates that RFID infrastructure will be rolled out to cover the top 39 POEs (in terms of number of travelers).

[52] This project is to enable IDENT backend services, such as IDENT watch list checks and enrollment in US-VISIT, to customers with mobile capability requirements.

Establishing Mutually Reinforcing or Joint Strategies

On July 31, 2006, the DHS Secretary established SCO to, among other things, coordinate and integrate the department's screening and credentialing efforts and create unified screening standards and policies. In July 2007, SCO issued a framework to help ensure the integration and alignment of screening programs. In short, the framework is to help identify opportunities for convergence and synergy among the related programs, as well as improvements in efficiency and mission effectiveness by providing a common method or process for the collection and use of data across these programs. According to the coordination office, the framework will eventually include a transition plan, including major activities, milestones, and associated time lines and costs. The SCO Associate Director told us that a draft transition plan is currently being reviewed within the department. The SCO is also the portfolio manager for the EA's screening/watchlist portfolio and, as such, works closely with the DHS Enterprise Architecture Board[53] (EAB) to ensure that its investments (e.g., those related to screening activities) are aligned with the EA and that the investments' resources are shared and effectively leveraged. However, as mentioned above, the EA is still evolving and does not define key aspects of the program's relationships and dependencies. Moreover, we have previously reported that DHS processes for ensuring that programs are aligned with its EA are not grounded in an explicit risk-based methodology and associated compliance criteria.

Leveraging Resources

In May 2007, the DHS Chief Information Officer and the SCO Director jointly issued a memo that, among other things, directed all programs that collect and use fingerprints when determining an individual's eligibility for entry or benefits to use US-VISIT's IDENT. In particular, programs were directed to provide the US-VISIT program office with their respective requirements for biometric vetting and storage. In doing so, DHS's aim is to leverage its IDENT resource as a shared capability or service for all DHS programs. Nevertheless, it is not clear that other opportunities to leverage resources across US-VISIT, WHTI, and SBI*net* are being exploited because doing so depends in large part on defining program-to-program relationships and plans for implementing SCO's screening framework, which have yet to be fully defined.

[53] The DHS EAB acts as the Executive Steering Committee for DHS IT programs and has the primary responsibility to oversee the department's EA.

Agreeing on Roles and Responsibilities

Certain department-level roles and responsibilities have been defined and agreed upon. As mentioned above, for example, SCO is responsible for coordinating the department's screening and credentialing programs and creating unified screening standards and policies, and has developed a framework and, according to the SCO Associate Director, a draft transition plan for achieving this. Also, the EAB is responsible for ensuring that DHS investments are aligned with the department's EA and that the investments' resources are shared and leveraged. However, as also mentioned above, program-level relationships, which would include roles and responsibilities for implementing the framework and interacting with related programs, have yet to be defined.

Establishing Compatible Policies, Procedures, and Other Means to Operate Across Organizational Boundaries

The department has established several mechanisms for facilitating how the US-VISIT, WHTI, and SBI*net* programs interact and operate with one another. For example, the DHS EA serves as a common frame of reference for programs to map to in an effort to minimize duplication and promote capability, and DHS's process for determining program alignment is intended to facilitate this. To illustrate, documentation from US-VISIT's most recent EA alignment review shows that the DHS Enterprise Architecture Center of Excellence[54] raised questions about the program's efforts to coordinate capabilities with other DHS programs, including SBI*net*. However, the EA is still evolving as a means for managing related programs, such as US-VISIT, WHTI, and SBI*net*. For example, US-VISIT's representation in the EA business model—which associates the department's business functions with the organizations that support and/or implement them—does not align US-VISIT with certain business functions (e.g., verify identity and establish identity) that the program office identifies as a critical part of its mission. Additionally, the EA does not associate US-VISIT with all the data systems that it owns and manages, and it does not define all system interfaces for IDENT. For example, the EA identifies ADIS and IDENT as being owned by CBP and ICE, respectively, even though both systems are owned by the US-VISIT program office. Also, it does not identify the interface between IDENT and GES, even though US-VISIT officials confirm that the interface exists and

[54] The DHS Enterprise Architecture Center of Excellence is responsible for conducting reviews of program alignment, technology insertions, service insertions and other decision requests to ensure alignment with the department's enterprise architecture. It is composed of members from the components including CBP and US-VISIT as well as specialty reviewers such as the Privacy Office.

is operating. According to the DHS Chief Architect, the next version of the EA is to address such inaccuracies.

Another mechanism to support interaction across programs is the SCO, which provides a means to coordinate and integrate the department's screening and credentialing activities, including a framework that provides for having a common method or process for collecting and using data. In addition, the coordination office provides other means for coordinating screening programs, such as weekly meetings with other programs. Specifically, SCO sponsors, and US-VISIT participates in, a weekly meeting to discuss WHTI implementation. According to the SCO Director, SCO also provides budget formulation and policy development advice to screening/watchlist portfolio programs to help limit overlap and redundancies and to leverage resources among programs.

At the program level, the US-VISIT program office has established a standard protocol for sending biometric information to and from IDENT and has developed interface control agreements to describe how the protocol will be used with other organizations.

Developing Mechanisms to Monitor, Evaluate, and Report on Results

SCO, through the EA draft transition plan, has developed performance indicators for the screening/watchlist portfolio. Such indicators include reducing the number of false positives from screening operations and increasing the use of technology to verify legitimacy of credentials. However, the data to be collected to implement such measures have not been defined.

Conclusions

The success of US-VISIT depends in large part on how well the program is defined, economically justified, and coordinated with related immigration and border management programs. While DHS has addressed each of these areas to some degree, none have been performed in a manner that fully reflects relevant federal guidance and related best practices, even though the program is now into its sixth year of activity, and more than a billion dollars has been invested in it. Of particular concern is that, after 5 years and tens of millions of dollars, DHS has yet to fully define and economically justify a comprehensive exit capability, including a plan describing what the capability will be, and how, when, and at what cost it will be delivered. Further, the Unique Identity component of the US-VISIT solution was not economically justified in a timely fashion to determine whether it was the most cost-effective solution before committing tens of millions of dollars. Therefore, DHS continues to lack a clear and fully defined strategic direction for how it will deliver on all its strategic program goals, and it continues to invest in the program without first knowing that its decision will produce cost effective and affordable results.

To DHS's credit, it has appropriately selected fingerprints as the biometric of choice for US-VISIT. Further, it has taken positive steps to coordinate US-VISIT with related immigration and border management programs, which provide the department opportunities to better reflect important collaboration practices.

Recommendations for Executive Action

To ensure that US-VISIT's strategic solution, including a comprehensive exit solution, is better defined, economically justified, and coordinated, we recommend that the Secretary of Homeland Security take the following two actions:

- Direct the Undersecretary for National Protection and Programs to have the US-VISIT Program Director
    - develop a plan for a comprehensive exit capability, which includes, at a minimum, a description of the capability to be deployed, the cost of developing, deploying and operating the capability, identification of key stakeholders and their respective roles and responsibilities, key milestones, and measurable performance indicators; and
    - develop an analysis of costs, benefits, and risks for proposed exit solutions before large sums of money are committed on those solutions, and use the analysis in selecting the final solution.
- Direct the appropriate DHS parties involved in defining, managing, and coordinating relationships across the department's border and immigration management programs to address the program collaboration shortcomings identified in this report, such as fully defining the relationships between US-VISIT and other immigration and border management programs and, in doing so, to employ the collaboration practices discussed in this report.

Agency Comments and Our Evaluation

In written comments on a draft of this report, signed by the Director, Departmental GAO/Office of Inspector General Liaison and reprinted in appendix IV, the department stated that it generally agreed with our observations and concurred with our recommendations.

In addition, the department stated that it has initiated actions to implement our recommendations. With respect to our recommendation to develop a plan and cost-benefit analysis for a comprehensive exit capability, DHS stated that the department remains committed to deploying an air exit solution by December 2008 and has completed a cost-benefit analysis for air and sea exit implementation. It is important that this cost-benefit analysis be used in selecting the final exit solution to ensure that the solution selected achieves the expected performance goals with the lowest life cycle costs and the least risk.

Regarding our recommendation to define, manage, and coordinate relationships across the department's border and immigration management programs, DHS stated that US-VISIT, along with appropriate parties, is developing and implementing an internal DHS governance board, which will include senior executives from programs such as WHTI and SBI, and which will provide a forum for collaboration and communication about the program. DHS also noted that, as part of its strategic planning efforts, US-VISIT solicits input from stakeholders such as DHS headquarters, CBP, ICE, and other federal agencies. DHS also stated that US-VISIT is integrally involved in departmental working groups on WHTI, SBI, and other immigration reform efforts. We support DHS's efforts in this area and emphasize the need for DHS to continue to implement the collaboration practices discussed in this report.

DHS also provided technical comments, which we have incorporated into this report as appropriate.

As we agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. We will then send copies of this report to the Chairmen and Ranking Members of the Senate and House Appropriations Committees and other Senate and House committees and subcommittees that have authorization and oversight responsibilities for homeland security. We will also send copies to the Secretary of Homeland Security and the Director of the Office of Management and Budget. We will also make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at www.gao.gov.

Should you or your offices have any questions on matters discussed in this report, please contact me at (202) 512-6222 or at willemssenj@gao.gov. Contact points for our Offices of Congressional Relations and Public

Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix V.

Joel Willemssen

Joel C. Willemssen
Managing Director, Information Technology Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine: (1) whether the Department of Homeland Security (DHS) has defined a strategic solution for meeting U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) goals and whether the solution has been economically justified; (2) the biometric technology options DHS has considered and the basis for the selected options; and (3) DHS's efforts to define, manage, and coordinate the relationships between US-VISIT and other immigration and border management programs.

To determine whether DHS has defined a strategic solution, we reviewed key program documentation, such as the US-VISIT strategic plan and implementation blueprint, program master schedule, program road map, Unique Identity project documentation (e.g., concept of operations, business requirements, system architectures, work breakdown structures, and project plans), and a high-level schedule for air exit. In doing so, we focused on determining such key factors as what program activities were planned, when and how they were to be accomplished, what resources were needed to accomplish them, and how they related to the program's strategic goals. We also interviewed program office officials and the Under Secretary for National Protection and Programs Directorate to obtain their views on the nature, content, and timing of the strategic solution. In cases where we were told of US-VISIT activities and capabilities that were not included in program documentation, we sought clarifications and plans for providing missing information. We also met with representatives from the U.S. Citizenship and Immigration Services (USCIS) to understand how that agency was implementing enumeration services.

To determine whether the strategic solution had been economically justified, we requested documentation of any economic analyses that had been developed. We received and reviewed the Unique Identity cost-benefit analysis, dated August 2006, and compared it with key Office of Management and Budget criteria.[1] However, a new analysis was completed in October 2007 and provided to us on November 30, 2007. We did not evaluate this analysis because it was not germane to the findings of this report. However, we interviewed program officials to understand the purpose and timing of this revised cost-benefit analysis.

[1] Office of Management and Budget, *Guidelines and Discount Rates for Benefits–Cost Analysis of Federal Programs, Circular A-94* (Washington, D.C.: Oct. 29, 1992).

To examine the biometric technology options DHS has considered and the basis for its selected option, we reviewed documentation from DHS, US-VISIT, National Institute of Standards and Technology (NIST), and the Department of Justice. In particular, we reviewed the Homeland Security Council's National Strategy for Homeland Security, DHS's Biometric Coordination Group charter, US-VISIT's Unique Identity Concept of Operations, NIST's 2003 Fingerprint Vendor Technology Evaluation, and a 2003 report to the Congress on the "Use of Technology Standards and Interoperable Databases With Machine-Readable, Tamper-Resistant Travel Documents," which was submitted by NIST, the Attorney General, and the Secretary of State. We also reviewed the Department of Justice's Inspector General's "Follow-up Review of the Federal Bureau of Investigation's Progress Toward Biometric Interoperability Between the Integrated Automated Fingerprint Identification System and the Automated Biometric Identification System." To understand how the information in these documents pertained to the program's biometric development efforts, we interviewed knowledgeable officials from the program office, DHS's Science & Technology Directorate, USCIS, and NIST. We also reviewed our past work on the use of biometrics in border security.[2] Finally, we analyzed relevant laws related to the requirements for US-VISIT's use of biometrics, including the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) and Enhanced Border Security and Visa Entry Reform Act of 2002.

To identify DHS's efforts to define, manage, and coordinate the relationship between US-VISIT and other immigration and border management programs, we identified department and program-level efforts taken to coordinate US-VISIT with these programs. In particular, we reviewed the latest version of the DHS enterprise architecture[3] to determine the extent to which it identifies the relationships between these programs and interviewed DHS's Chief Architect to determine how the architecture is used to manage these relationships. We also reviewed DHS strategic planning documents, as well as DHS's Screening Coordination Office's Credentialing Framework. We interviewed representatives of the Screening Coordination Office to determine what actions are being taken to coordinate screening programs.

[2] GAO, *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174 (Washington, D.C.: Nov. 15, 2002).

[3] Homeland Security EA 2007.

We then compared actions taken with selected key practices that our research has found can enhance and sustain agencies' collaborative efforts,[4] focusing on those practices that were particularly relevant and applicable to our objective. These practices include the following:

- establishing common outcomes;
- establishing mutually reinforcing or joint strategies;
- leveraging resources;
- agreeing on roles and responsibilities;
- establishing a compatible means to operate across organizational boundaries; and
- developing mechanisms to monitor, evaluate, and report on results.

To assess data reliability, we reviewed quality and access controls of the systems used to generate the data. We also reviewed related program documentation to substantiate data provided in interviews with knowledgeable agency officials. We have also made appropriate attribution indicating the data's sources. When we found data to be unreliable or did not assess the data's reliability, we annotated the data as such.

We conducted our work at DHS headquarters offices in Washington, D.C., the US-VISIT Program Office in Rosslyn, Virginia, and NIST headquarters offices in Gaithersburg, Maryland. Our work was conducted from January 2007 through January 2008 in accordance with generally accepted government auditing standards.

[4] GAO-06-15.

Appendix II: Overview of Legislative Underpinnings for the US-VISIT Program

A series of federal statutes have provided a framework for the strategic focus of the US-VISIT program. The first of these statutes dates back to more than a decade ago, and the latest law was passed in 2007. The statutes are summarized here.

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996[1] required the development of an automated entry and exit control system to collect a record of departure for every alien departing the United States and then match the record of departure with the record of the alien's arrival in the United States; make it possible, through online searching procedures, to identify nonimmigrants who remain in the country beyond the authorized period; and integrate the overstay information into appropriate databases of the former Immigration and Naturalization Service[2] and the Department of State, including those used at air, sea, and land ports of entry (POE) and at consular offices. The system was to be developed by September 30, 1998; however, the act was amended to change this deadline to October 15, 1998,[3] and was amended again to change the deadline for land border POEs and seaports to March 30, 2001.[4]

The Immigration and Naturalization Service Data Management Improvement Act of 2000[5] replaced the 1996 statute in its entirety. Specifically, the act required an electronic system that would provide access to and integrate alien arrival and departure data that are authorized or required to be created or collected under law, are in an electronic format, and are in a database of the Department of Justice or the Department of State, including those created or used at POEs and at consular offices. The act specifically provided that it not be construed to permit the imposition of any new documentary or data collection requirements on any person for the purpose of satisfying its provisions, but it further provided that it also not be construed to reduce or curtail any authority of the Attorney General (now Secretary of Homeland

[1] Pub. L. No. 104-208, div. C, sec. 110 (Sept. 30, 1996).

[2] Effective March 1, 2003, the Immigration and Naturalization Service became part of DHS.

[3] Pub. L. No. 105-259 (Oct. 15, 1998).

[4] Pub. L. No. 105-277 (Oct. 21, 1998).

[5] Pub. L. No. 106-215 (June 15, 2000).

Security)[6] or Secretary of State under any other provision of law. The integrated entry and exit data system was to be implemented at airports and seaports by December 31, 2003, at the 50 busiest land POEs by December 31, 2004, and at all remaining POEs by December 31, 2005.

The act also required that the system use available data to produce an annual report of arriving and departing aliens by country of nationality, classification as an immigrant or nonimmigrant, and timeliness of departure from the United States. The system was to match an alien's available arrival data with the alien's available departure data, assist in the identification of possible overstays, and use available alien arrival and departure data for annual reports to the Congress. These reports were to include the number of aliens for whom departure data was collected during the reporting period, with an accounting by country of nationality; the number of departing aliens whose departure data was successfully matched to the alien's arrival data, with an accounting by country of nationality and classification as an immigrant or nonimmigrant; the number of aliens who arrived pursuant to a nonimmigrant visa, or as a visitor under the Visa Waiver Program, for whom no matching departure data have been obtained as of the end of the alien's authorized period of stay, with an accounting by country of nationality and date of arrival in the United States; and the number of identified overstays, with an accounting by country of nationality.

The USA PATRIOT Act of 2001[7] provided that, in developing the integrated entry and exit data system, the Secretary of Homeland Security and Secretary of State were to focus particularly on the utilization of biometric technology and the development of tamper-resistant documents readable at POEs. It also required that the system be able to interface with law enforcement databases for use by federal law enforcement to identify and detain individuals who pose a threat to the national security of the United States.

The USA PATRIOT Act also required by October 26, 2003, the development and certification of a technology standard, including appropriate biometric

[6] The Homeland Security Act of 2002 transferred the border patrol, detention and removal, intelligence, investigations, and inspections programs previously under the Department of Justice's Commissioner of Immigration and Naturalization to DHS's Under Secretary for Border and Transportation Security. 6 U.S.C. § 251.

[7] Pub. L. No. 107-56 (Oct. 26, 2001).

identifier standards, that could be used to verify the identity of persons applying for a U.S. visa or persons seeking to enter the United States pursuant to a visa for the purposes of conducting background checks, confirming identity, and ensuring that a person has not received a visa under a different name. This technology standard was to be the technological basis for a cross-agency, cross-platform electronic system that is a cost-effective, efficient, fully interoperable means to share law enforcement and intelligence information necessary to confirm the identity of persons applying for a U.S. visa or persons seeking to enter the United States pursuant to a visa. This electronic system was to be readily and easily accessible to consular officers, border inspection agents, and law enforcement and intelligence officers responsible for investigation or identification of aliens admitted to the United States pursuant to a visa. Every 2 years beginning on April 26, 2003, the Secretary of Homeland Security and the Secretary of State were to jointly report to the Congress on the development, implementation, efficacy, and privacy implications of the technology standard and electronic database system.

The Visa Waiver Permanent Program Act[8] required DHS to develop and implement a fully automated system to control entry and exit of aliens at airports and seaports who enter the United States under the Visa Waiver Program. The act also required that, by October 1, 2002, inspectors at the POEs have access to Department of State and DHS information to determine whether an alien is eligible to be admitted into the United States or to receive a visa. Further, the act required that visa waiver applicants be checked against watch list systems, and, that by October 1, 2003, aliens applying for a visa waiver have a machine-readable passport.[9] The act was subsequently amended to require, not later than August 3, 2008, an exit system using biometric information and recording the departure on a flight leaving the United States of every alien participating in the Visa Waiver Program.[10]

[8] Pub. L. No. 106-396 (Oct. 30, 2000).

[9] Between October 1, 2003, and September 30, 2007, the Secretary of State could waive the requirement for machine readable passports if the country (1) was making progress toward ensuring that machine-readable passports are generally available to its nationals and (2) it has taken appropriate measures to protect against misuse of passports it issued that do not meet the requirements.

[10] 8 U.S.C. § 1187(i).

The Enhanced Border Security and Visa Entry Reform Act of 2002[11] required that, in developing the integrated entry and exit data system for the POEs, the Secretary of Homeland Security and Secretary of State implement, fund, and use the technology standard required by the USA PATRIOT Act at U.S. POEs and at consular posts abroad. The act amended the USA PATRIOT Act to move up the date for the development and certification of the technology standard to January 26, 2003, and moved up the date for the biannual reports to the Congress on the technology standard to October 26, 2002. The 2002 act also required the Secretary of Homeland Security and Secretary of State to establish a database containing the arrival and departure data from machine-readable visas, passports, and other travel and entry documents possessed by aliens and make interoperable all security databases relevant to making determinations of admissibility under section 212 of the Immigration and Nationality Act. In implementing these requirements, DHS and the Department of State were to utilize technologies that facilitate the lawful and efficient cross-border movement of commerce and persons without compromising the safety and security of the United States and were to consider implementing a North American National Security Program, for which other provisions in the act called for a feasibility study.

The act, as amended, also established a number of requirements regarding biometric travel and entry documents. It required that, not later than October 26, 2004, the Secretary of Homeland Security and the Secretary of State issue to aliens only machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers and that they jointly establish document authentication standards and biometric identifiers standards to be employed on such visas and other travel and entry documents from among those biometric identifiers recognized by domestic and international standards organizations. It also required by October 26, 2004 (amended to October 26, 2005), the installation at all U.S. POEs equipment and software to allow biometric comparison and authentication of all U.S. visas and other travel and entry documents issued to aliens and passports issued by visa waiver participants. Such biometric data readers and scanners were to be those that domestic and international standards organizations determine to be highly accurate when used to verify identity, that can read the biometric identifiers used under the act, and that can authenticate the document presented to verify

[11] Pub. L. No. 107-173 (May 14, 2002).

identity. These systems also were to utilize the technology standard established pursuant to the USA PATRIOT Act.

The Intelligence Reform and Terrorism Prevention Act of 2004[12] described the program as an "automated biometric entry and exit data system" and required DHS to develop a plan to accelerate the full implementation of the program and to report to the Congress on this plan by June 15, 2005. The report was to provide several types of information about the implementation of US-VISIT,[13] including a "listing of ports of entry and other Department of Homeland Security and Department of State locations with biometric exit data systems in use." The report also was to provide a description of the manner in which the US-VISIT program "meets the goals of a comprehensive entry and exit screening system, including both entry and exit biometrics;" and fulfills the statutory obligations imposed on the program by several laws enacted between 1996 and 2002. The act provided that US-VISIT "shall include a requirement for the collection of biometric exit data for all categories of individuals who are required to provide biometric entry data, regardless of the port of entry where such categories of individuals entered the United States."

The provisions in the 2004 act also addressed other areas related to US-VISIT, such as the integration and interoperability of databases and data systems that process or contain information on aliens and federal law enforcement and intelligence information relevant to visa issuance and admissibility of aliens and maintenance of the accuracy and integrity of the US-VISIT data system. It further addressed using US-VISIT to track and facilitate the processing of immigration benefits using biometric identifiers; the goals of the program (e.g., serving as a vital counterterrorism tool, screening visitors efficiently and in a welcoming manner, integrating relevant databases and plans for database modifications to address volume increase and database usage, and providing inspectors and related personnel with adequate real-time information); and training, education, and outreach on US-VISIT, low-risk visitor programs, and immigration law. Finally, it addressed annual compliance reports by DHS, the Department of State, the Department of Justice, and any other department or agency subject to the requirements of

[12] Pub. L. No. 108-458 (Dec. 17, 2004).

[13] On April 29, 2003, the Secretary of DHS renamed the entry exit system the US-VISIT system.

the new provisions; and development and implementation of a registered traveler program.

Appendix III: Overview of Biometric Technologies

Biometric identification systems are human characteristic pattern recognition systems. While the biometric technologies used in these systems vary in complexity, capabilities, and performance, the technologies all share several elements. They use acquisition devices, such as cameras and scanning devices, to capture images, recordings, or measurements of an individual's characteristics and computer hardware and software to extract, encode, store, and compare these characteristics. Because the process is automated, biometric comparison is generally very fast, in most cases taking only a few seconds in real time.

Depending on the application, biometric systems can be used in one of two modes: identification or verification. Identification is referred to as one-to-many matching because an individual's presented biometric is compared against the stored biometric templates[1] of all individuals enrolled in the system. Verification—also called authentication—is referred to as one-to-one matching because an individual's presented biometric is compared against the biometric for that person, which was stored in the system during enrollment.

How Biometrics Work

Biometric technologies are available today and are being used for a variety of applications, such as access control, criminal identification, and border security. While several biometric technologies are in use or being proposed, the more common technologies and the ones that the US-VISIT program office considered for its strategic solution are fingerprint recognition, facial recognition, and iris recognition.

When used for personal identification, biometric technologies measure and analyze human physiological and behavioral characteristics. Identifying a person's physiological characteristics is based on direct measurement of a part of the body, such as fingertips, faces, and irises. The corresponding biometric technologies are fingerprint, facial, and iris recognition. Identifying a person's behavioral characteristics is based on data derived from actions, such as speech and signature, the corresponding biometrics being speaker recognition and signature recognition.

[1] After a biometric system extracts the features of an individual's body part, it uses an algorithm to encode the features and store the information in a biometric template that can be used for future comparison.

Biometrics are theoretically effective personal identifiers because the characteristics they measure are thought to be distinct to each person. Unlike conventional identification methods that use something you have, such as an identification card to gain access to a building, or something you know, such as a password to log on to a computer system, these characteristics are intrinsic to who you are. Because they are inherent in an individual, they are more reliable, cannot be forgotten, and are less easily lost, stolen, or guessed.

Although biometric technologies measure different characteristics in substantially different ways, all biometric systems involve similar processes that can be divided into two distinct stages: enrollment and identification or verification. No match is ever perfect in either an identification or a verification system because every time a biometric is captured, the template is likely to be unique. Therefore, biometric systems can be configured to make a match or no-match decision, based on a predefined number, referred to as a threshold, which establishes the acceptable degree of similarity between the trial template and the enrolled reference template. After the comparison, a score representing the degree of similarity is generated, and this score is compared with the threshold to make a match or no-match decision. For algorithms for which the similarity between two templates is calculated, a score exceeding the threshold is considered a match. For algorithms for which the difference between two templates is calculated, a score below the threshold is considered a match. Depending on the setting of the threshold in identification systems, several reference templates can be considered matches to the trial template, with the better scores corresponding to better matches.

Types of Biometric Technologies

As mentioned above, the three biometric technologies that the US-VISIT program office considered for its strategic solution are fingerprint recognition, facial recognition, and iris recognition. These three technologies are discussed in the sections that follow.

Fingerprint Recognition

Fingerprint recognition technology[2] extracts features from impressions made by the distinct ridges on the fingertips. The fingerprints can be either

[2] Fingerprint recognition is one of the best known and most widely used biometric technologies. Automated systems have been commercially available since the early 1970s, and there are currently more than 75 fingerprint recognition technology companies. Until recently, it was used primarily in law enforcement applications.

flat or rolled. A flat print captures only an impression of the central area between the fingertip and the first knuckle; a rolled print captures ridges on both sides of the finger. An image of the fingerprint is captured by a scanner, enhanced, and converted into a template. Scanner technologies can be optical, silicon, or ultrasound technologies, with optical being the most commonly used. During enhancement, the definition of the ridges is augmented to offset such things as dirt, cuts, scars, and creases or dry, wet, or worn fingerprints. Template size ranges from 250 bytes up to 1,000 bytes, depending on which vendor's proprietary algorithm the system uses. Approximately 80 percent of vendors base their algorithms on the extraction of minutiae points relating to breaks in the ridges of the fingertips. Other algorithms are based on extracting ridge patterns.

Facial Recognition

Facial recognition technology identifies people by analyzing features of the face not easily altered—the upper outlines of the eye sockets, the areas around the cheekbones, and the sides of the mouth. The technology is typically used to compare a live facial scan to a stored template, but it can also be used in comparing static images such as digitized passport photographs. Facial recognition can be used in both identification and verification systems. In addition, because facial images can be captured from video cameras, facial recognition is the only biometric that can be used for surveillance purposes.

Iris Recognition

Iris recognition technology focuses on the distinctly colored ring surrounding the pupil of the eye. Made from elastic connective tissue, the iris is a very rich source of biometric data, having approximately 266 distinctive characteristics. Formed during the eighth month of gestation, these characteristics reportedly remain stable throughout a person's lifetime, except in cases of injury. Iris recognition systems use a small, high-quality camera to capture a black-and-white, high-resolution image of the iris. They then define the boundaries of the iris, establish a coordinate system over the iris, and define the zones for analysis within the coordinate system. The visible characteristics within the zones are then converted into a 512-byte template that is used to identify or verify the identity of an individual.

Using Biometrics to Enroll Individuals

In enrollment, a biometric system is trained to identify a specific person. The person first provides an identifier, such as an identification document. That person then presents the biometric (e.g., fingertips, face, or iris) to an acquisition device, and the biometric is linked to his or her identity. Depending on the technology, the biometric sample may be collected as an image, a recording, or a record of related dynamic measurements.

Template size also varies, depending on the vendor and the technology, and can be stored remotely in a central database or within a biometric reader device itself; their small size also allows for storage on smart cards or tokens.

Minute changes in positioning, distance, pressure, environment, and other factors influence the generation of a template, making each template likely to be unique, each time an individual's biometric data are captured and a new template is generated. Consequently, depending on the biometric system, a person may need to present biometric data several times in order to enroll. The reference template may then either represent an amalgam of the captured data or several enrollment templates may be stored. The quality of the template or templates is critical in the overall success of the biometric application. Because biometric features can change over time, people may have to reenroll to update their reference template. Some technologies can update the reference template during matching operations.

The enrollment process also depends on the quality of the identifier the enrollee presents. The reference template is linked to the identity specified on the identification document. If the identification document does not specify the individual's true identity, the reference template will be linked to a false identity.

Using Biometrics to Identify Individuals

In identification systems, the purpose is to identify who the person is. To find a match, the trial template is compared against the stored reference templates of all individuals enrolled in the system. Identification systems are referred to as one-to-many matching because an individual's biometric is compared against multiple biometric templates in the system's database.

There are two types of identification systems: positive and negative. Positive identification systems are designed to ensure that an individual's biometric is enrolled in the database. The anticipated result of a search is a match. A typical positive identification system controls access to a secure building or secure computers by checking anyone who seeks access against a database of enrolled employees. The goal is to determine whether a person seeking access can be identified as having been enrolled in the system.

Negative identification systems are designed to ensure that a person's biometric information is not present in a database. The anticipated result of a search is a nonmatch. Comparing a person's biometric information against a database of all who are registered in a public benefits program, for example, can ensure that this person is not "double dipping" by using fraudulent documentation to register under multiple identities.

Another type of negative identification system is a surveillance system that uses a watch list. Such systems are designed to identify people on the watch list and alert authorities for appropriate action. For all other people, the system is to check that they are not on the watch list and allow them normal passage. The people whose biometrics are in the database in these systems may not have provided them voluntarily. For instance, for a surveillance system, the biometrics may be faces captured from mug shots provided by a law enforcement agency.

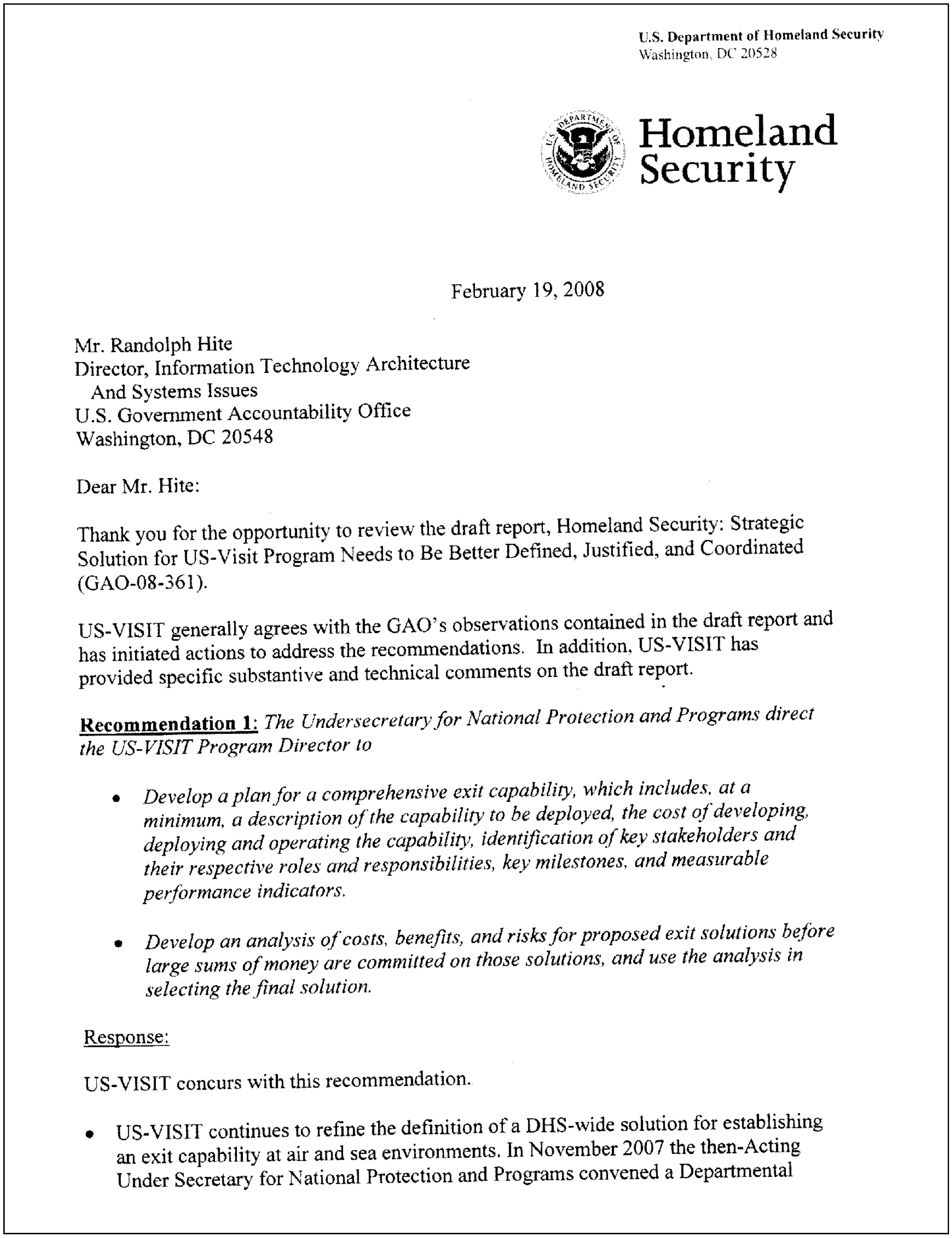
Using Biometrics to Verify Individuals

In verification systems, the purpose is to verify that a person is who he or she claims to be (i.e., the person who enrolled). After the individual provides the identifier he or she used to enroll, the biometric is presented, which the biometric system captures, generating a trial template that is based on the vendor's algorithm. The system then compares the trial biometric template with this person's reference template, which was stored in the system during enrollment, to determine whether the individual's trial and stored templates match.

Verification is often referred to as one-to-one matching. Verification systems can contain databases ranging from dozens to millions of enrolled templates but are always predicated on matching an individual's presented biometric against his or her reference template. Nearly all verification systems can render a match or no-match decision in less than a second. An example of a verification application is a system that requires employees to authenticate their claimed identities before granting them access to secure buildings or to computers.

US-VISIT functions both as an identification system and a verification system. In the case of identification, US-VISIT serves as a negative identification system by utilizing watchlist information, such as the Federal Bureau of Investigation's Criminal Master File, to identify individuals that should be denied entry into the United States and possibly apprehended or detained by law enforcement officials. In the case of verification, US-VISIT is used to verify the identities of travelers who have been enrolled in the system.

Appendix IV: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

February 19, 2008

Mr. Randolph Hite
Director, Information Technology Architecture
And Systems Issues
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Hite:

Thank you for the opportunity to review the draft report, Homeland Security: Strategic Solution for US-Visit Program Needs to Be Better Defined, Justified, and Coordinated (GAO-08-361).

US-VISIT generally agrees with the GAO's observations contained in the draft report and has initiated actions to address the recommendations. In addition, US-VISIT has provided specific substantive and technical comments on the draft report.

Recommendation 1: *The Undersecretary for National Protection and Programs direct the US-VISIT Program Director to*

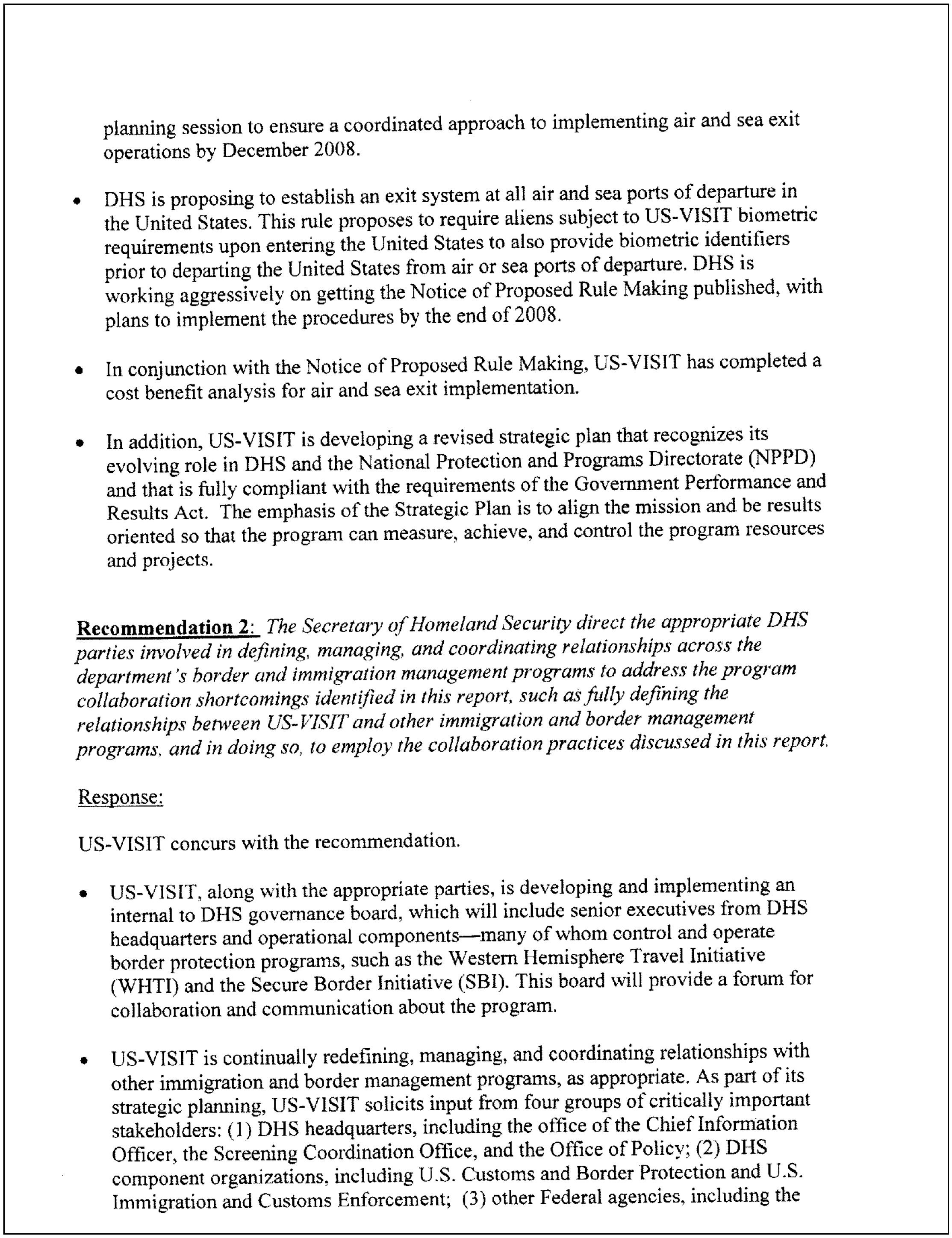
- *Develop a plan for a comprehensive exit capability, which includes, at a minimum, a description of the capability to be deployed, the cost of developing, deploying and operating the capability, identification of key stakeholders and their respective roles and responsibilities, key milestones, and measurable performance indicators.*

- *Develop an analysis of costs, benefits, and risks for proposed exit solutions before large sums of money are committed on those solutions, and use the analysis in selecting the final solution.*

Response:

US-VISIT concurs with this recommendation.

- US-VISIT continues to refine the definition of a DHS-wide solution for establishing an exit capability at air and sea environments. In November 2007 the then-Acting Under Secretary for National Protection and Programs convened a Departmental



planning session to ensure a coordinated approach to implementing air and sea exit operations by December 2008.

- DHS is proposing to establish an exit system at all air and sea ports of departure in the United States. This rule proposes to require aliens subject to US-VISIT biometric requirements upon entering the United States to also provide biometric identifiers prior to departing the United States from air or sea ports of departure. DHS is working aggressively on getting the Notice of Proposed Rule Making published, with plans to implement the procedures by the end of 2008.

- In conjunction with the Notice of Proposed Rule Making, US-VISIT has completed a cost benefit analysis for air and sea exit implementation.

- In addition, US-VISIT is developing a revised strategic plan that recognizes its evolving role in DHS and the National Protection and Programs Directorate (NPPD) and that is fully compliant with the requirements of the Government Performance and Results Act. The emphasis of the Strategic Plan is to align the mission and be results oriented so that the program can measure, achieve, and control the program resources and projects.

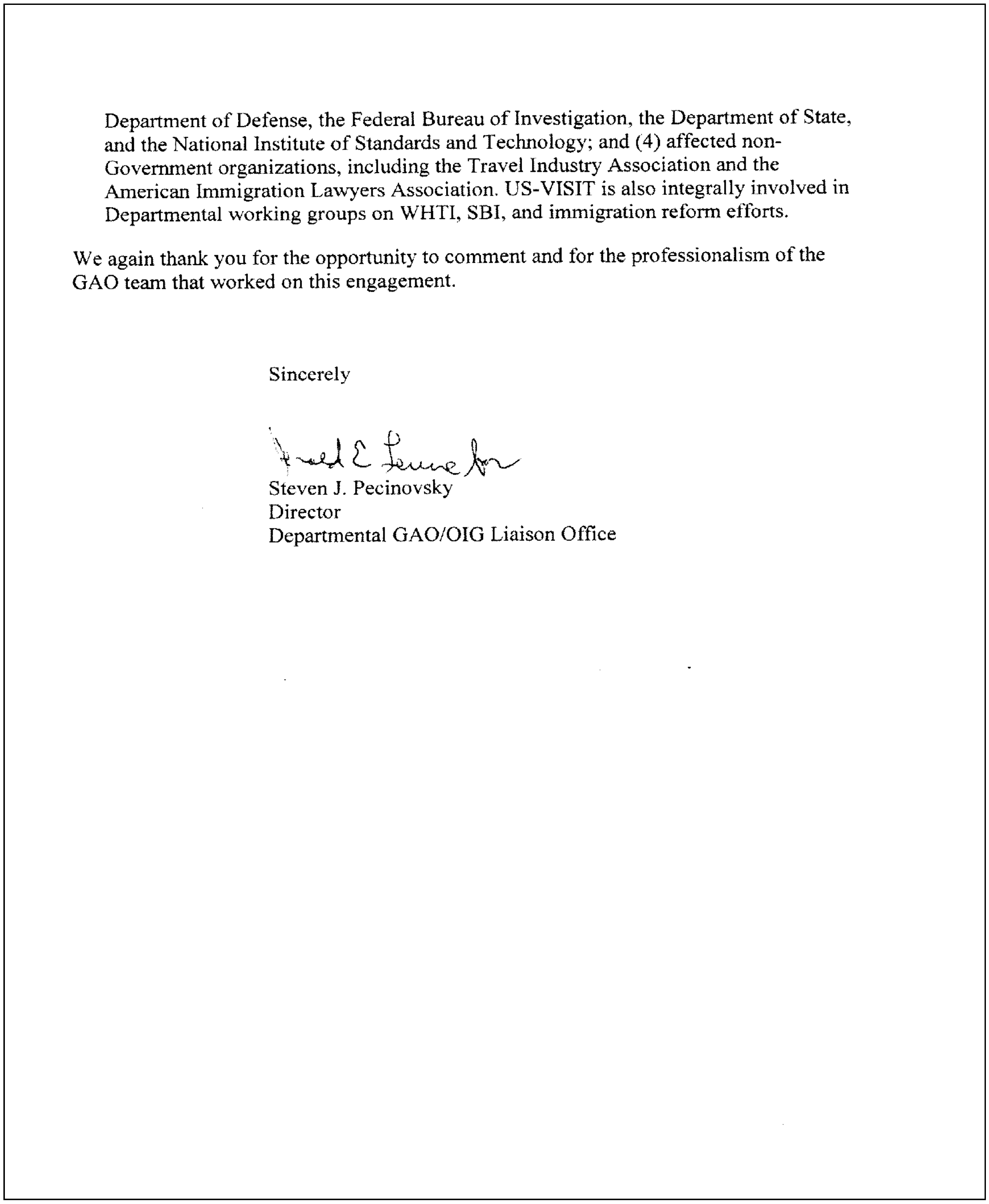
Recommendation 2: *The Secretary of Homeland Security direct the appropriate DHS parties involved in defining, managing, and coordinating relationships across the department's border and immigration management programs to address the program collaboration shortcomings identified in this report, such as fully defining the relationships between US-VISIT and other immigration and border management programs, and in doing so, to employ the collaboration practices discussed in this report.*

Response:

US-VISIT concurs with the recommendation.

- US-VISIT, along with the appropriate parties, is developing and implementing an internal to DHS governance board, which will include senior executives from DHS headquarters and operational components—many of whom control and operate border protection programs, such as the Western Hemisphere Travel Initiative (WHTI) and the Secure Border Initiative (SBI). This board will provide a forum for collaboration and communication about the program.

- US-VISIT is continually redefining, managing, and coordinating relationships with other immigration and border management programs, as appropriate. As part of its strategic planning, US-VISIT solicits input from four groups of critically important stakeholders: (1) DHS headquarters, including the office of the Chief Information Officer, the Screening Coordination Office, and the Office of Policy; (2) DHS component organizations, including U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement; (3) other Federal agencies, including the



Department of Defense, the Federal Bureau of Investigation, the Department of State, and the National Institute of Standards and Technology; and (4) affected non-Government organizations, including the Travel Industry Association and the American Immigration Lawyers Association. US-VISIT is also integrally involved in Departmental working groups on WHTI, SBI, and immigration reform efforts.

We again thank you for the opportunity to comment and for the professionalism of the GAO team that worked on this engagement.

Sincerely

Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison Office

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Joel C. Willemssen, (202) 512-6222, or willemssenj@gao.gov

Staff Acknowledgments

In addition to the individual named above, Deborah Davis, Assistant Director; Harold Brumm; Neil Doherty; Kory Godfrey; Matthew Grote; Joshua Hammerstein; Dave Hinchman; Sandra Kerr; Kaelin Kuhn; Nicholas Marinos; Madhav Panwar; Sushmita Srikanth; Amos Tevelow; Jessica Waselkow; and Eric Winter made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

PRINTED ON ♻ RECYCLED PAPER