

GAO

Testimony

Before the Committee on Government
Reform, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Thursday, September 9, 2004

BORDER SECURITY

Joint, Coordinated Actions by State and DHS Needed to Guide Biometric Visas and Related Programs

Joint Statement of Jacquelyn L. Williams-Bridgers,
Managing Director, International Affairs and Trade, and
Randolph Hite, Director of Information Technology
Architecture and Systems Issues



GAO
Accountability • Integrity • Reliability

Highlights

Highlights of [GAO-04-1080T](#), a testimony before the Committee on Government Reform, House of Representative

Why GAO Did This Study

Since September 11, 2001, the U.S. government has made a concerted effort to strengthen border security by enhancing visa issuance policies and procedures, as well as expanding screening of the millions of foreign visitors who enter the United States annually. Consistent with the 9/11 Commission report that recommends a biometric entry-exit screening system for travelers, the Department of State's biometric program complements the Department of Homeland Security's (DHS) United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program—a governmentwide program to better control and monitor the entry, visa status, and exit of visitors.

GAO was asked to present the findings of its report on State's Biometric Visa Program, as well as discuss other aspects of visa processing and border security that require coordinated, joint actions by State and DHS.

What GAO Recommends

GAO has recommended that DHS and State develop and provide guidance to consular posts on how to use information from the biometric program to adjudicate visas. In other reports, GAO has made recommendations to DHS and State to improve US-VISIT, as well as several aspects of the nonimmigrant visa process. The agencies generally agreed and are taking actions to implement our recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-04-1080T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Jacquelyn L. Williams-Bridgers at (202) 512-4128 or williamsbridgersj@gao.gov.

BORDER SECURITY

Joint, Coordinated Actions by State and DHS Needed to Guide Biometric Visas and Related Programs

What GAO Found

Our report issued today finds that State is implementing the Biometric Visa Program on schedule and will likely meet the October 26, 2004, deadline for issuing visas that include biometric indicators, as mandated by Congress. As of September 1, 2004, State had installed program hardware and software at 201 visa issuing posts overseas and plans to complete the installation at the remaining 6 posts by September 30. Technology installation has progressed smoothly, however State and DHS have not provided comprehensive guidance to consular posts on when and how information from the DHS Automated Biometric Identification System (IDENT) on visa applicants should be considered by adjudicating consular officers. In the absence of such guidance, we found that these officers are unclear on how best to use the biometric program and IDENT information.

Since September 11, State and DHS have made many improvements to visa issuance and border security policies. Nevertheless, in prior reports, we have found additional vulnerabilities that need to be addressed through joint, coordinated actions. For example, DHS has not adequately defined the operational context for US-VISIT, which affects the biometric program. In addition, we identified systemic weaknesses in information sharing between State and DHS in the visa revocation process. Moreover, we found related weaknesses in an interagency security check process aimed to prevent the illegal transfer of sensitive technologies.

Example of Fingerprints and Photograph Capture

Bio Capture Window

Applicant Data

Case Number: 00000000
Surname: DOE
Given Name: JOAN
DOB: 1/1/50 POB: Natl: Gender: F

Photo

Fingerprint 1

Fingerprint 2

Freeze

Cancel

Close

Right Index

Left Index

Ready for photo and fingerprint capture

Data updated successfully

5/18/04 3:15 pm

Source: GAO analysis of State data.

Mr. Chairman and Members of the Committee:

We are pleased to be here to discuss our report¹ being issued today on the Department of State's Biometric Visa Program, which requires that all persons applying for U.S. visas have certain biometrics² (in this case, fingerprints) and digital photographs collected during the visa³ application process and cleared through the Department of Homeland Security's (DHS) Automated Biometric Identification System (IDENT) before receiving a visa. In addition, we will discuss several previous GAO reports that highlight the need for joint, coordinated efforts by State and DHS on programs to enhance border security and visa processes.

Since September 11, 2001, the U.S. government has made a concerted effort to strengthen border security by enhancing visa issuance policies and procedures, as well as improving the screening of the millions of foreign visitors who enter, stay in, and exit the United States annually. State's Biometric Visa Program complements the DHS-run United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program—a governmentwide program that collects, maintains, and shares information on foreign nationals to better control and monitor the entry, visa status, and exit of visitors. The Biometric Visa Program prescreens visa applicants at U.S. consulates overseas to ensure that they are qualified to obtain visas, while the US-VISIT program, among other things, verifies that the same person who applied for a visa is the one who is entering the United States using that visa.⁴ The biometric program is consistent with

¹See GAO, *BORDER SECURITY: State Department Rollout of Biometric Visas on Schedule, but Guidance Is Lagging*, [GAO-04-1001](#) (Washington, D.C.: Sept. 9, 2004).

²Biometrics is a wide range of technologies that can be used to, among other things, verify a person's identity by capturing and analyzing his or her physiological characteristics. In this case, and for the purposes of this report, "biometric identifiers" refers to fingerprints. See GAO, *Technology Assessment: Using Biometrics for Border Security*, [GAO-03-174](#) (Washington, D.C.: Nov. 14, 2002).

³In this report, we use the term "visa" to refer to nonimmigrant visas only. The United States also grants visas to people who intend to immigrate to the United States. A visa allows a foreign visitor to present himself at a port of entry for admission to the United States.

⁴DHS currently does not have information on individuals apprehended at ports of entry when their prints and photographs did not match those captured at the consular posts for the visa they were using. On July 19, 2004, DHS implemented a system to assist in identifying such cases and indicated that it will be able to develop better information in the future.

the July 2004 9/11 Commission report,⁵ which recommends using biometric identifiers for border and transportation systems and a biometric entry-exit screening system for travelers.

Our statement today will focus on border security programs requiring joint, coordinated efforts by State and DHS. We will first discuss our observations of State's Biometric Visa Program. In addition, based on prior GAO reports, we will discuss some of our findings and our recommendations that called for coordinated efforts between DHS and State to improve other aspects the nonimmigrant visa process (NIV) and border security, including US-VISIT.

Summary

We found that State is implementing the Biometric Visa Program on schedule and will likely meet the October 26, 2004, deadline for issuing visas with biometric identifiers, as mandated by Congress.⁶ As of September 1, 2004, State had installed program hardware and software at 201 of 207 overseas posts that issue visas, and State plans to complete the installation at the remaining 6 posts by September 30. The biometric technology installation has progressed smoothly; however, DHS and State have not provided comprehensive guidance to consular posts on when and how information from IDENT on visa applicants should be considered by adjudicating consular officers.⁷ In the absence of such guidance, officers may be unclear on how best to use the biometric program and IDENT information. Therefore, in our report issued today, we have recommended that DHS and State develop and provide comprehensive guidance to consular posts on how information on visa applicants available through

⁵The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, D.C.: July 22, 2004).

⁶Section 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 State Department issue visas that use biometric identifiers.

⁷The Homeland Security Act of 2002 establishes DHS's role in the visa process, and a subsequent September 2003 Memorandum of Understanding between the Secretaries of State and Homeland Security further outlines the visa issuance authorities. According to the memorandum, DHS is responsible for establishing visa policy, reviewing implementation of the policy, and providing additional direction, while State is responsible for managing the visa process, managing the consular corps and its functions, and carrying out U.S. foreign policy. DHS and State share responsibility for policy and implementation of the Biometric Visa Program.

IDENT should be used to help adjudicate visas. DHS concurred with our report, and State acknowledged that there may be a lag in guidance.

State and DHS have made many improvements to border security and visa issuance policies since September 11, 2001. Nevertheless, in our reviews of various aspects of border security and visa issuance, we have found weaknesses that both agencies need to address through joint, coordinated actions. For example,

- DHS has deployed an initial US-VISIT operating capability for entry to 115 airports and 14 seaports. DHS plans to expand the initial operating capability to the 50 busiest land ports of entry by December 2004, and to all remaining land ports of entry by December 2005. It has also deployed an exit capability, on a pilot basis, at two airports and one seaport.⁸ However, the program's operational context, or homeland security enterprise architecture,⁹ has not yet been adequately defined.¹⁰ DHS released an initial version of its enterprise architecture in September 2003; however, we found that this architecture was missing important content. This content is needed to help clarify and optimize the relationships between US-VISIT and other homeland security programs and operations, such as State's Biometric Visa Program.
- In 2003, we identified systemic weaknesses in the visa revocation process,¹¹ many of which were the result of a failure of U.S. agencies to share and fully utilize information.¹² We reported that information on

⁸These are the Baltimore/Washington International Airport, Chicago O'Hare International Airport, and the Miami Royal Caribbean seaport.

⁹An enterprise architecture provides a clear and comprehensive picture of the structure of an entity, whether an organization or a functional or mission area, including depictions of the enterprise's current or "as-is" technical and operational environments, its target or "to-be" technical and operational environments, and a plan for transitioning to the target. A properly managed enterprise architecture can clarify and help optimize the interdependencies and relationships among business operations, as well as those between these operations and the underlying information technology infrastructure and applications.

¹⁰See GAO, *Homeland Security: Efforts Are Underway to Develop Enterprise Architecture, But Much Work Remains*, [GAO-04-777](#) (Washington, D.C.: Aug. 6, 2004).

¹¹The visa revocation process is a homeland security tool that can prevent potential terrorists from entering the United States and can help DHS officials identify and investigate potential terrorists that may have already entered the country.

¹²See GAO, *BORDER SECURITY: New Policies and Procedures Are Needed to Fill Gaps in the Visa Revocation Process*, [GAO-03-798](#) (Washington, D.C.: June 18, 2003).

individuals with visas revoked on terrorism grounds was not shared between State and appropriate immigration and law enforcement offices. We made several recommendations to State and DHS, which they agreed to implement. A follow-up review in summer 2004, showed that although State and DHS had made improvements in the revocation process, some weaknesses remained.¹³ For instance, in some cases State took a week or longer to notify DHS that individuals with revoked visas might have been in the country. As a result, we made additional recommendations to both agencies, which they agreed to implement.

- Timely information sharing among State, DHS, and other agencies also affects the time it takes to adjudicate a visa for a science student or scholar. In some cases, consular officers determine that some of these applicants must undergo a security check, known as Visas Mantis, to protect against sensitive technology transfers.¹⁴ In February 2004, we found that it was difficult to resolve some Visas Mantis cases expeditiously given the way in which information was disseminated among State, DHS, and other agencies.¹⁵ Again, we addressed recommendations to both State and DHS, and they are currently implementing them.

Overall, our work has demonstrated that joint, coordinated actions by State and DHS are critical for homeland and border security.

Background

State's \$162 million Biometric Visa Program is designed to work hand-in-hand with the DHS multibillion-dollar US-VISIT program. Both programs aim to improve U.S. border security by verifying the identity of persons entering the United States. Both programs rely on the DHS Automated Biographic Identification System, known as IDENT, which is a repository of fingerprints and digital photographs of persons who either have applied for U.S. visas since the inception of the program in September 2003, have entered the United States at one of 115 air or 14 sea ports of entry since

¹³See GAO, *BORDER SECURITY: Additional Actions Needed to Eliminate Weaknesses in the Visa Revocation Process*, [GAO-04-795](#) (Washington, D.C.: July 13, 2004).

¹⁴The Visas Mantis process allows all participating agencies, including DHS, to provide information and raise any particular concerns that they may have regarding the applicant and/or the applicant's proposed activities in the United States. According to State, the key role of the Visas Mantis process is to protect U.S. national security, particularly in combating the proliferation of weapons of mass destruction, their delivery systems, and conventional weapons.

¹⁵See GAO, *BORDER SECURITY: Improvements Needed to Reduce Time Taken to Adjudicate Visas for Science Students and Scholars*, [GAO-04-371](#) (Washington, D.C.: Feb. 25, 2004).

January 2004, or are on a watch list—whether for previous immigration violations or as part of the FBI’s database of terrorists and individuals with felony convictions.¹⁶

Biometric Process at U.S. Consulates Overseas

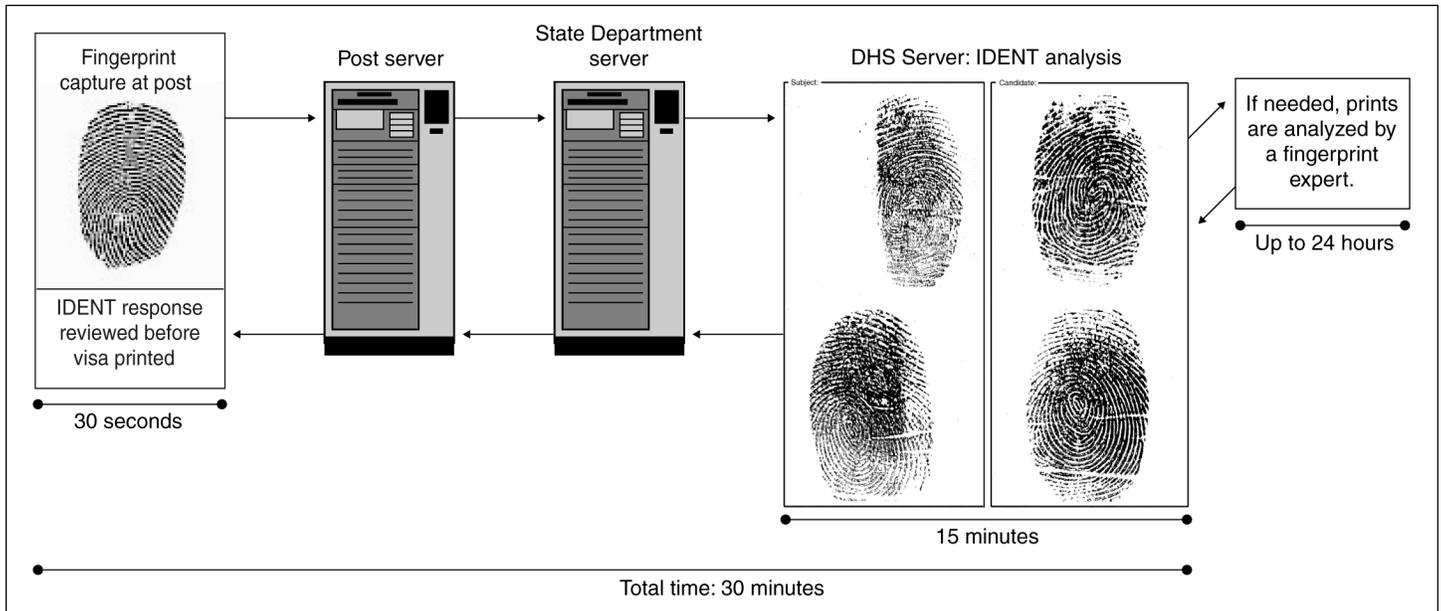
The process for determining who will be issued a visa consists of several steps. When a person applies for a visa at a U.S. consulate, a fingerprint scan is taken of his right and left index fingers. These prints are then transmitted from the overseas post through servers¹⁷ at State to DHS’s IDENT system, which searches its records and sends a response back through State to the post.¹⁸ A “hit” response—meaning that a match to someone previously entered in the system was found—prevents the post’s computer system from printing a visa for the applicant until the information is reviewed and cleared by a consular officer. According to State data, the entire process generally takes about 30 minutes. If the computer cannot determine if two sets of prints match, IDENT refers the case to DHS fingerprint experts, who have up to 24 hours to return a response to State (see fig. 1).

¹⁶IDENT data includes 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 Immigration and Customs Enforcement information on deported felons and sexual registrants; and DHS information on previous criminal histories. Information from the bureau includes fingerprints from the Integrated Automated Fingerprint Identification System.

¹⁷A server is a computer on a network that manages network resources, such as storing files, managing printers, managing network traffic, or processing database queries

¹⁸In a hit record, information is included on the person’s previous entry in the system, either at a port of entry or U.S. consulate, or through the watch list.

Figure 1: Biometric Fingerprint Analysis Process



Sources: GAO analysis of State and DHS processes.

United States Visitor and Immigrant Status Indicator Technology Program

US-VISIT aims to enhance national security, facilitate legitimate trade and travel, contribute to the integrity of the U.S. immigration system, and adhere to U.S. privacy laws and policies 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 traveler identity, and determining traveler admissibility through the use of biometrics; and
- facilitating information sharing and coordination among appropriate agencies.

The process by which a foreign national is screened for entry is as follows: When a foreign national arrives at a port of entry to the United States, a DHS inspector scans the machine-readable travel documents. Existing records on the foreign national, including biographic lookout hits are returned. The computer presents available biographic information and a photograph and determines whether IDENT contains existing fingerprints for the foreign national. The inspector then scans the foreign national's fingerprints (left and right index fingers) and takes a photograph. This information is checked against stored fingerprints in IDENT. If no matching prints are in IDENT, the foreign national is enrolled in US-VISIT (i.e., biographic and biometric data are entered). If the foreign national's fingerprints are already in IDENT, the system performs a comparison of the fingerprint taken at the port of entry to the one on file to confirm that the person submitting the fingerprints is the person on file. If the system finds a mismatch of fingerprints or a watch list hit, the foreign national is held for further screening or processing.

Biometric Visa Implementation Nearing Completion, but Some Guidance Still Needed

State's implementation of the technology aspects of the biometric visa program is currently on schedule to meet the October 26, 2004, deadline. According to State officials, a well-planned rollout of equipment and software and fewer technical problems than anticipated led to smooth implementation of the technological aspects of the program at the 201 posts that had the program operating as of September 1, 2004. But amid the fast pace of rolling out the program to meet the deadline, DHS and State have not provided comprehensive guidance for consular posts on how the information about visa applicants made available through the Biometric Visa Program should best be used to help adjudicate visas. Indeed, we found several significant differences in the implementation of the biometric program during our visits to San Salvador, El Salvador, and Santo Domingo, Dominican Republic. State acknowledged that posts may be implementing the program in various ways across the 207 consular posts that issue nonimmigrant visas.

State Expects to Meet Implementation Deadline

According to State officials, the implementation process for the biometric program led to far fewer technical problems than expected. Early on, State had a few difficulties in transmitting data between the posts and DHS's IDENT, primarily related to server and firewall (computer security) issues. According to State, most issues were resolved within a few days. In fact, 201 nonimmigrant visa (NIV)-issuing posts out of 207 had the software and hardware installed and were transmitting prints to IDENT for analysis as

of September 1, 2004. State anticipates the completion of the installation by the October 2004 deadline.

Fingerprinting Raising Issues in Visa Process

According to State's data, from February to August 2004, the total biometric visa process averaged about 30 minutes for an applicant's prints to be sent from an overseas post to the State server, and on to DHS for IDENT analysis and then for the response to be returned through State's server to the posts. IDENT response time could affect visa issuance times because a visa cannot be issued until the post has received and reviewed the IDENT response. Our observations at posts in San Salvador and Santo Domingo demonstrated the importance of the length of time required to receive an IDENT response. We observed that most interviews average only a few minutes, but the IDENT response time currently is 30 minutes. Thus, if interviewing officers collect prints during the interview, the interview would be completed before the IDENT response would be available to consular officers. Since the visa cannot be issued until the IDENT information is considered by the consulate, potential delays in the IDENT response times could have a major effect on the visa issuance process and inconvenience visa applicants. State has encouraged consular officials to issue visas the day after interviews since part of the visa process now relies on another agency's system. This will require significant changes for posts such as Santo Domingo, which still issues same-day visas.

Guidance Lagging for Program Implementation

State has focused on implementing the Biometric Visa Program by the mandated deadline; however, our report identifies certain lags in guidance on how the program should be implemented at consular posts. State and DHS have not yet provided to posts details of how all aspects of the program will be implemented, including who should scan fingerprints, where and who should review information about applicants returned from IDENT, and response times for the IDENT system. In addition, DHS and State have not provided comprehensive guidance for consular posts on how the information about visa applicants made available through the Biometric Visa Program should be used to help adjudicate visas.

We believe that it is important for State and DHS to articulate how the program could best be implemented, providing a roadmap for posts to develop implementation plans that incorporate the guidance. We recognize, however, that the workload, personnel and facility resources vary considerably from post to post. As a result, each post may not be able to easily implement the Biometric Visa Program according to a precise set

Program Implementation Varies at Consular Posts

of guidelines. However, posts could develop procedures to implement the guidance, identify resource and facility constraints, and implement mitigating actions to address their own unique circumstances. Therefore, we have recommended that DHS and State provide comprehensive guidance to consular posts on how information about visa applicants that is now available from IDENT should be used to help adjudicate visas. In responding to our recommendation, DHS generally concurred and State acknowledged that there may be a lag in guidance.

Our work at two posts shows that, because they lack specific guidance on the system's use, consular officers at these overseas posts are uncertain how they should implement the Biometric Visa Program and are currently using the returned IDENT responses in a variety of ways. For example, we found that, in cases in which the IDENT response information is available to the overseas post by the time of the visa applicant interview, some consular officers who conduct interviews review information before the interview, some review it during the interview, and some rely instead on a designated officer or the line chief to review the information after the interview is completed and before affected visas are printed.

We found several differences in the visa operations at two posts—San Salvador, El Salvador, and Santo Domingo, Dominican Republic—that handle a large volume of visa applications. For example,

- San Salvador, one of the first posts to begin implementing the program in September 2003, has a large new embassy complex that allowed the post great flexibility in implementing the collection of biometrics. Applicants are led through outdoor security screening before entering the interview waiting room. Once in the waiting room, they immediately proceed to a fingerprint scanning window where an American officer verifies their names and photographs and scans their fingerprints. By the time they arrive at their interview windows, usually the interviewing officer has received their IDENT responses. However, the post has designated one officer to review all of the IDENT responses, so some interviewing officers do not take the time to review IDENT information on those they interview even if the information is available at the time of the interview.
- Santo Domingo's consular section is hampered by significant facility constraints. The NIV applicant waiting area is very cramped and has been even more restricted over recent months due to construction efforts. Some of the NIV applicants are forced to share space in the immigrant visa waiting area. Santo Domingo has fewer interviewing windows than San Salvador and cannot easily spare one to designate for fulltime fingerprint

scanning due to high interview volume. Some interviewing officers scan applicants' fingerprints at the time of the interview, so the interview ends before the IDENT response has been returned from DHS. One consular officer is designated to review the IDENT responses for all of the applicants, and interviewing officers may not see IDENT information on the applicants they interview. In some cases, the designated officer determines if the applicant should receive a visa, and in others he brings the IDENT information back to the original interviewing officer for the case for further review.

Joint, Coordinated Actions by State and DHS Required on Many Aspects of Visa Processing and Border Security

Since September 11, 2001, we have issued reports recommending that State and DHS work together to improve several aspects of border security and the visa process, as described below. These reports show the importance of joint, coordinated actions by State and DHS to maximize program effectiveness.

US-VISIT Operating at Selected Points of Entry, but DHS Further Defining its Operational Context

The US-VISIT program supports a multifaceted, critical mission: to help protect approximately 95,000 miles of shoreline and navigable waterways through inspections of foreign nationals at U.S. ports of entry. DHS has deployed an initial operating capability for entry to 115 airports and 14 seaports. It has also deployed an exit capability, as a pilot, at two airports and one seaport. Since becoming operational, DHS reports that more than eight million foreign nationals have been processed by US-VISIT at ports of entry, resulting in hundreds being denied entry. Its scope is large and complex, connecting 16 existing information technology systems in a governmentwide process involving multiple departments and agencies.¹⁹ In addition to these and other challenges, the program's operational context, or homeland security enterprise architecture, is not yet adequately defined.

DHS released an initial version of its enterprise architecture in September 2003; however, we found that this architecture was missing, either

¹⁹GAO has identified US-VISIT as a high-risk endeavor. See GAO, *Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed*, [GAO-03-1083](#) (Washington, D.C.; Sept. 19, 2003).

partially or completely, all the key elements expected in a well-defined architecture, such as descriptions of business processes, information flows among these processes, and security rules associated with these information flows.²⁰ DHS could benefit from such key elements to help clarify and optimize the relationships between US-VISIT and other homeland security programs operations, such as State's Biometric Visa Program, both in terms of processes and the underlying information technology infrastructure and applications. Although the biometrics program is administered by State, it falls under the overall visa policy area of the DHS Directorate of Border and Transportation Security, and is part of our national homeland security mission. State officials indicated that they are waiting for DHS to further define US-VISIT, which would help guide State's actions on the Biometric Visa Program.

Aspects of NIV Process Require State and DHS Cooperation

Since September 11, 2001, our work has demonstrated the need for State and DHS to work together to better address potential vulnerabilities in the visa process. In June 2003, we identified systemic weaknesses in the visa revocation process, many of which were the result of a failure to share and fully utilize information. We reported that the visa revocation process was not used aggressively to share information among agencies on individuals with visas revoked on terrorism grounds.²¹ It also broke down when these individuals had already entered the United States prior to revocation. Immigration officials and the Federal Bureau of Investigation (FBI) were not then routinely taking actions to investigate, locate, or resolve the cases of individuals who remained in the United States after their visas were revoked. Therefore, we recommended that DHS, in conjunction with the Departments of State and Justice, develop specific policies and procedures to ensure that appropriate agencies are notified of revocations based on terrorism grounds and take proper actions.

In July 2004, we followed up on our findings and recommendations regarding interagency coordination in the visa revocation process and found that State and DHS had taken some actions in the summer of 2003 to address these weaknesses.²² However, our review showed that some weaknesses remained. For instance, in some cases State took a week or

²⁰DHS plans to release an updated version of its enterprise architecture in September 2004.

²¹[GAO-03-798](#).

²²[GAO-04-795](#).

longer to notify DHS that individuals with revoked visas might be in the country. Without these notifications, DHS may not know to investigate those individuals. Given outstanding legal and policy issues regarding the removal of individuals based solely on their visa revocation, we recommended that the Secretaries of Homeland Security and State jointly (1) develop a written governmentwide policy that clearly defines roles and responsibilities and sets performance standards and (2) address outstanding legal and policy issues in this area or provide Congress with specific actions it could take to resolve them. State agreed to work together with DHS to address these recommendations.

In February 2004, we reported that the time it takes to adjudicate a visa for a science student or scholar depends largely on whether an applicant must undergo a security check known as Visas Mantis, which is designed to protect against sensitive technology transfers.²³ Based on a random sample of Visas Mantis cases for science students and scholars, we found it took an average of 67 days for the interagency security check to be processed and for State to notify the post. We also found that the way in which Visas Mantis information was disseminated at headquarters made it difficult to resolve some cases expeditiously. Finally, consular staff at posts we visited stated that they lacked clear guidance on the Visas Mantis program. While State and FBI officials acknowledged there had been lengthy waits, they reported having measures under way to improve the process and to identify and resolve outstanding Visas Mantis cases. We recommended that the Secretary of State, in coordination with the Director of the FBI and the Secretary of Homeland Security, develop and implement a plan to improve the Visas Mantis process. We are currently reviewing the measures these agencies have taken to improve the Visas Mantis program made since our February report and will report on our findings at the beginning of next year.

Overall, we have reported on a number of areas in which joint, coordinated actions by DHS and State are needed to improve border security and visa processing. In commenting in our report of State's biometric program, both DHS and State have pledged their commitment to continued cooperation and joint actions. Indeed, these agencies are currently working together as part of the US-VISIT program. For example, State participates in two DHS-led groups designed to oversee and manage the US-VISIT program. First, State participates on the US-VISIT Federal

²³[GAO-04-371](#).

Stakeholders Advisory Board, which provides guidance and direction to the US-VISIT program. State also participates as part of the US-VISIT Integrated Project Team, which meets weekly to discuss, among other things, operational issues concerning the deployment of US-VISIT.

Conclusion

Mr. Chairman, overall, our work has demonstrated that coordinated, joint actions by State and DHS are critical for homeland and border security. State and DHS have worked together to roll out the biometric technology to consular posts worldwide on schedule. Moreover, their cooperation on US-VISIT will be critical to ensure that information is available to consulates to adjudicate visa applications and prevent persons from unlawfully entering the United States. However, they have not yet provided comprehensive guidance to the posts on how the program and biometric information should be used to adjudicate visas. We recognize that it may not be feasible for each post to implement biometric visas in the same way, given the variances among posts in workload, security concerns with the applicant pool, facilities, and personnel. However, guidance to posts on how to best implement the program, including best practices, would enable posts to develop operating procedures, identify resource needs, and implement mitigating actions to address the unique circumstances at each post.

Therefore we have recommended that the Secretaries of Homeland Security and State develop and provide comprehensive guidance to consular posts on how best to implement the Biometric Visa Program. The guidance should address the planned uses for the information generated by the Biometric Visa Program at consular posts including directions to consular officers on when and how information from the IDENT database on visa applicants should be considered. Further, we have recommended that the Secretary of State direct consular posts to develop an implementation plan based on this guidance. DHS generally concurred with our recommendations, stating that GAO's identification of areas where improvements are needed in the Biometric Visa Program will contribute to ongoing efforts to strengthen the visa process. State acknowledged that there may be a lag in guidance. Regarding US-VISIT, we made an earlier recommendation that the Secretary for Homeland Security clarify the operational context in which US-VISIT is to operate. DHS agreed with our recommendation and plans to issue the next version of their enterprise architecture in September of 2004. This is an essential component in establishing biometric policy and creating consistency between the DHS-run US-VISIT program and State's Biometric Visa program.

Mr. Chairman, this concludes my prepared statement. I would be pleased to answer any questions you or other members of the committee may have.

Contacts and Acknowledgments

For questions regarding this testimony, please call Jess Ford at (202) 512-4128. Other key contributors to this statement include John Brummet, Sharron Candon, Deborah Davis, Kathryn Hartsburg, David Hinchman, and David Noone.

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

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 "Subscribe to 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, D.C. 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

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548