United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Terrorism, Technology, and Homeland Security and Subcommittee on Border Security, Immigration, and Citizenship, Committee on the Judiciary, United States Senate

For Release on Delivery
Expected at 10:00 a.m. EST
Wednesday March 12, 2003

BORDER SECURITY

Challenges in Implementing Border Technology

Statement of Nancy Kingsbury, Managing Director
Applied Research and Methods

Mr. Chairmen and Members of the Subcommittees:

I appreciate the opportunity to participate in today's hearing on border technology. The Department of Homeland Security (DHS) faces enormous challenges to protect the nation from terrorism.[1] One of the primary missions of the new department focuses on border control – preventing the illegal entry of people and goods into the United States. Part of this mission is controlling the passage of travelers through official ports of entry into the United States. Facilitating the flow of people while preventing the illegal entry of travelers requires an effective and efficient process that authenticates a traveler's identity. Generally, identifying travelers at the ports of entry is performed by inspecting their travel documents, such as passports and visas, and asking them questions. Technologies called biometrics can automate the identification of individual travelers by one or more of their distinct physiological characteristics. Biometrics have been suggested as a way of improving the nation's ability to determine whether travelers are admissible to the United States. Today, I will discuss the issues and challenges associated with using biometrics in border control systems and the significant management challenges we identified during our ongoing work at land ports of entry.

My testimony today is based on a body of work we completed last year examining the use of biometrics for border control and on preliminary observations related to our ongoing work examining the inspection of travelers at land border ports of entry. In our report on the use of biometrics, we discussed the current maturity of several biometric technologies, the possible implementation of these technologies in current border control processes, and the policy implications and key considerations for using these technologies.[2] We are also in the process of reviewing immigration inspections at land border ports of entry, where our work has included examining the integrity of the inspections process, programs to segregate low-risk travelers, the technology and equipment

[1] We recently designated the implementation and transformation of DHS as a high-risk area due in part to the inherited operational and management challenges faced by the department. See U.S. General Accounting Office, *Major Management Challenges and Program Risks: Department of Homeland Security*, GAO-03-102 (Washington D.C.: Jan. 2003).

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

used to conduct inspections, immigration intelligence information, and inspector training issues.

In brief, biometric technologies are available today that can be used for border control. However, questions remain regarding the technical and operational effectiveness of biometric technologies in applications as large as border control. Before implementing any biometric border control system, a number of other issues would have to be considered, including the system's effect on existing border control procedures and people, the costs and benefits of the system, and the system's effect on privacy, convenience, and the economy. Furthermore, technology is only part of the solution. Effective security requires technology and people to work together to implement policies, processes, and procedures. At land border ports of entry, DHS faces several challenges including ensuring that the inspections process has sufficient integrity to enable inspectors to intercept those who should not enter our country, while still facilitating the entry of lawful travelers; ensuring that inspectors have the necessary technology, equipment, and training to do their job efficiently and effectively; and providing inspectors the access to necessary intelligence information.

Background

The United States essentially relies on a two-step process to prevent inadmissible people from entering the country. The Bureau of Consular Affairs in the State Department is responsible for issuing international travel documents, such as passports to United States citizens and visas to citizens of other countries. On March 1, 2003, the Bureau of Customs and Border Protection in the Department of Homeland Security assumed responsibility for inspecting travelers at and between ports of entry. Inspectors from the Immigration and Naturalization Service (INS), the U.S. Customs Service, and the Animal and Plant Health Inspection Service (APHIS) were brought together in this new bureau.

In fiscal year 2002, there were about 440 million border crossings into the United States at over 300 designated ports of entry (see table 1). Of the more than 358 million border crossers who entered through land ports of entry, almost 50 million entered as pedestrians. The rest entered in more than 131 million vehicles, including cars, trucks, buses, and trains. Further, the State Department processed about 8.4 million nonimmigrant visa applications and issued about 7 million passports.

Table 1: Number of Inspections at U.S. Ports of Entry, Fiscal Year 2002

Type of port	Number of inspections
Sea	12,369,035
Air	69,679,190
Land	358,373,569
Total	**440,421,794**

Source: GAO analysis of INS data.

The term biometrics covers a wide range of technologies that can be used to verify a person's identity by measuring and analyzing his or her physiological characteristics, based on data derived from measuring a part of the body directly. For example, technologies have been developed to measure a person's finger, hand, face, retina, and iris. Biometric systems are essentially pattern recognition systems. They use electronic or optical sensors such as cameras and scanning devices to capture images, recordings, or measurements of a person's characteristics and computer hardware and software to extract, encode, store, and compare these characteristics.

Using biometrics as identifiers for border security purposes appears to be appealing because they can help tightly bind a traveler to his or her identity by using physiological characteristics. Unlike other identification methods, such as identification cards or passwords, biometrics are less easily lost, stolen, or guessed. The binding is dependent on the quality of the identification document presented by the traveler to enroll in the biometric system. If the identification document does not specify the traveler's true identity, the biometric data will be linked to a false identity.

Applying Biometrics to Border Control

In our work last year, we examined several different biometric technologies and found four to be suitable for border control systems: fingerprint recognition, facial recognition, iris recognition, and hand geometry. Other biometric technologies were determined to be impractical in a border control application because of accuracy or user acceptance issues. For example, speaker recognition systems do not perform well in noisy environments and do not appear to be sufficiently distinctive to permit identification of an individual within a large database of identities.

We defined four different scenarios in which biometric technologies could be used to support border control operations. Two scenarios use a biometric watch list to identify travelers who are inadmissible to the United States (1) before issuing travel documents and (2) before travelers

enter the country. The other two scenarios help bind the claimed identity of travelers to their travel documents by incorporating biometrics into (1) U.S. visas or (2) U.S. passports. Linking an individual's identity to a U.S. travel document could help reduce the use of counterfeit documents and imposters' fraudulent use of legitimate documents.

Biometrics have been used in border control environments for several years. For example, the INS Passenger Accelerated Service System (INSPASS), a hand geometry system first installed in 1993, has been used in seven U.S. and two Canadian airports to reduce inspection time for trusted travelers. Since April 1998, border crossing cards, also called laser visas, have been issued to Mexican citizens that include their photograph and prints of the two index fingers.[3] The Automated Biometric Fingerprint Identification System (IDENT) is used by DHS to identify aliens who are repeatedly apprehended trying to enter the United States illegally. IDENT is also being used as a part of the National Security Entry-Exit Registration System (NSEERS) that was implemented last year.[4]

Laws passed in the last 2 years require a more extensive use of biometrics for border control.[5] The Attorney General and the Secretary of State jointly, through the National Institute of Standards and Technology (NIST) are to develop a technology standard, including biometric identifier standards. When developed, this standard is to be used to verify the identity of persons applying for a U.S. visa for the purpose of conducting a background check, confirming identity, and ensuring that a person has not received a visa under a different name. By October 26, 2004, the Departments of State and Justice are to issue to aliens only machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers. At the same time, Justice is to install at all ports of entry equipment and software that allow the biometric comparison and

[3] Border crossing cards allow Mexican citizens to enter the United States for the purpose of business or pleasure without being issued further documentation and to stay for 72 hours or less within 25 miles of the U.S./Mexican border.

[4] Under NSEERS, certain nonimmigrants, who may pose a national security risk, are being registered, and are fingerprinted and photographed when they arrive in the United States. These nonimmigrants are required to periodically report and update, when changes occur, their registration information, and record their departure from the country.

[5] See the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) (Public Law 107-56, §403(c) and §414, Oct. 26, 2001) and the Enhanced Border Security and Visa Entry Reform Act of 2002 (Public Law 107-173, May 14, 2002).

authentication of all U.S. visas and other travel and entry documents issued to aliens and machine-readable passports.

Challenges and Implications to Applying Biometrics at the Border

While biometric technology is currently available and used in a variety of applications, questions remain regarding the technical and operational effectiveness of biometric technologies in applications as large as border control. In addition, before implementing any biometric border control system, a number of other issues would have to be considered including:

- The system's effect on existing border control procedures and people. Technology is only part of an overall security solution and only as effective as the procedures within which it operates.
- The costs and benefits of the system, including secondary costs resulting from changes in processes or personnel to accommodate the biometrics.
- The system's effect on privacy, convenience, and the economy.

Introducing Technology Affects People and Procedures

The successful implementation of any technology depends not only on the performance of the technology but also on the operational processes that employ the technology and the people who execute them. The implementation of biometrics in border security is no exception. Further, the use of technology alone is not a panacea for the border security problem. Instead, biometric technology is just a piece of the overall decision support system that helps determine whether to allow a person into the United States. The first decision is whether to issue travelers a U.S. travel document. The second decision, made at the ports of entry, is whether to admit travelers into the country. Biometrics can play a role in both decisions. Sorting the admissible travelers from the inadmissible ones is currently conducted by using information systems for checking names against watch lists and by using manual human recognition capabilities to see if the photograph on a travel document matches the person who seeks entry to the United States. When enabled with biometrics, automated systems can verify the identity of the traveler and assist inspectors in their decision making.

However, a key factor that must be considered is the performance of the biometric technology. For example, if the biometric technology that is used to perform watch list checks before visas are issued has a high rate of false matches, the visa processing workload could increase at the embassies and consulates. If the same biometric solution were used at the

ports of entry, it could lead to increased delays in the inspection process and an increase in the number of secondary inspections.

Exception processing will also have to be carefully considered. Exceptions would include people who fail to enroll in the biometric visa system or are not correctly matched by it. Exception processing that is not as good as biometric-based primary processing could be exploited as a security hole. Failure of equipment must also be considered and planned for. Further, to issue visas with biometrics, an appropriate transition strategy must be devised to simultaneously handle both visas with biometrics and the current visa that could remain valid without biometrics for up to the next 10 years.

Weighing Costs and Benefits

Before any significant project investment is made, the benefit and cost information of the project alternatives should be analyzed and assessed in detail. A clear statement of the high-level system goals should drive the overall concept of a U.S. border control system. System goals address the system's expected outcomes and are usually based on business or public policy needs, which for a border control system could include items such as binding a biometric feature to a person's identity on a travel document, identifying undesirable persons on a watch list, checking for duplicate enrollments in the system, verifying identities at the borders, ensuring the security of the biometric data, and ensuring the adequacy of privacy protections. The benefits gained from a biometric border control system should be based on how well the system achieves the high-level goals.

A concept of operations should be developed that embodies the people, process, and technologies required to achieve the goals. To put together the concept of operations, a number of inputs have to be considered, including legal requirements, existing processes and infrastructure used, and known technology limitations. Performance requirements should also be included in the concept of operations, such as processing times. Business process reengineering, such as new processes to conduct inspections of passengers in vehicles or to maintain a database of biometric data, would also be addressed in the concept of operations.

As we have noted, the desired benefit is the prevention of the entry of travelers who are inadmissible to the United States. More specifically, the use of a biometric watch list can provide an additional check to name-based checks and can help detect travelers who have successfully established separate names and identities and are trying to evade detection. The use of visas with biometrics can help positively identify

travelers as they enter the United States and can limit the use of fraudulent documents, including counterfeit and modified documents, and impostors' use of legitimate documents.

However, the benefits gained by using biometric have several limitations. First, the benefit achieved is directly related to the performance of the biometric technology. The performance of facial, fingerprint, and iris recognition is unknown for systems as large as a biometric visa system that would require storage and comparison against 100 million to 240 million records. The largest facial, fingerprint, and iris recognition systems contain 60 million, 40 million, and 30,000 records, respectively.

The population of the biometric watch list is critical to its effectiveness. Policies and procedures would need to be developed for adding and maintaining records in the watch list database. Key questions that have to be answered include who is added to the watch list, how someone is removed from the watch list, and how errors could be corrected. Successfully identifying people on the biometric watch list is also dependent on the effectiveness of the law enforcement and intelligence communities in identifying individuals who should be placed on the watch list.

Issuing visas with biometrics will only assist in identifying those currently required to obtain visas to enter this country. For example, Canadians, Mexicans with border crossing cards, and foreign nationals participating in the visa waiver program do not have to have a visa to enter the United States. The issuance of visas with biometrics is also dependent on establishing the correct identity during enrollment. This process typically depends on the presentation of identification documents. If the documents do not specify the applicant's true identity, then the travel document will be linked to a false identity.[6]

Further, biometric technology is not a solution to all border security problems. Biometric technology can address only problems associated with identifying travelers at official locations such as embassies and ports of entry. While the technology can help reduce the number of illegal immigrants who cross with fraudulent documents, it cannot help with

[6] We have previously reported on weaknesses in the visa issuing process. See U.S. General Accounting Office, *Border Security: Visa Process Should Be Strengthened as an Antiterrorism Tool*, GAO-03-132NI (Washington D.C.: Oct. 21, 2002).

illegal immigrants who cross between the ports of entry. INS has previously estimated that up to 60 percent of the 275,000 new illegal immigrants a year do not present themselves at a port of entry to enter the United States. In addition, biometrics cannot help to identify foreign nationals who enter through ports of entry and are properly admitted by an inspector but may overstay their visit.

The costs of any proposed system must be considered. Both initial costs and recurring costs need to be estimated. Initial costs need to account for the engineering efforts to design, develop, test, and implement the system; training of personnel; hardware and software costs; network infrastructure improvements; and additional facilities required to enroll people into the biometric system. Recurring cost elements include program management costs, hardware and software maintenance, hardware replacement costs, training of personnel, additional personnel to enroll or verify the identities of travelers in the biometric system, and possibly the issuance of token cards for the storage of biometrics collected for issuing visas. While specific cost estimates depend on the detailed assumptions made for the concept of operations, the costs are significant.

Effect on Privacy, the Economy, and International Relations

The Privacy Act of 1974 limits federal agencies' collection, use, and disclosure of personal information, such as fingerprints and photographs. Accordingly, the Privacy Act generally covers federal agency use of personal biometric information. However, as a practical matter, the act is likely to have a more limited application for border security. First, the act applies only to U.S. citizens and lawfully admitted permanent residents. Second, the act includes exemptions for law enforcement and national security purposes. Representatives of civil liberties groups and privacy experts have expressed concerns regarding (1) the adequacy of protections for security, data sharing, identity theft, and other identified uses of biometric data and (2) secondary uses and "function creep." These concerns relate to the adequacy of protections under current law for the large-scale data handling in a biometric system. Besides information security, concern was voiced about an absence of clear criteria for governing data sharing. The broad exemptions of the Privacy Act, for example, provide no guidance on the extent of the appropriate uses law enforcement may make of biometric information. Because there is no general agreement on the appropriate balance of security and privacy to build into a system using biometrics, further policy decisions are required. The range of unresolved policy issues suggests that questions surrounding

the use of biometric technology center as much on management policies as on technical issues.

The use of biometric technologies could potentially impact the length of the inspection process. Any lengthening in the process of obtaining travel documents or entering the United States could affect travelers significantly. At some consular posts, visas are issued the day applications are received. Even without biometrics, the busiest ports of entry regularly have delays of 2 to 3 hours. Increases in inspection times could compound these delays. Delays inconvenience travelers and could result in fewer visits to the United States or lost business to the nation. Further studies will be necessary to measure what the potential effect could be on the American economy and, in particular, on the border communities. These communities depend on trade with Canada and Mexico, which totaled $653 billion in 2000.

The use of biometrics in a border control system in the United States could affect the number of international visitors and how other countries treat visitors from the United States. Much visa issuance policy is based on reciprocity—that is, the process for allowing a country's citizens to enter the United States would be similar to the process followed by that country when U.S. citizens travel there. If the United States requires biometric identifiers when citizens of other countries apply for a visa, those countries may require U.S. citizens to submit a biometric when applying for a visa to visit their countries. Similarly, if the United States requires other countries to collect biometrics from their citizens and store the data with their passport for verification when they travel here, they may require the United States to place a biometric in its passports as well.

As more countries require the use of biometrics to cross their borders, there is a potential for different biometrics to be required for entering different countries or for the growth of multiple databases of biometrics. Unless all countries agree on standard biometrics and standard document formats, a host of biometric scanners might be required at U.S. and other ports of entry. The International Civil Aviation Organization plans to standardize biometric technology for machine-readable travel documents, but biometric data-sharing arrangements between the United States and other countries would also be required.

Issues Raised in Joint Report from Justice, State, and NIST

In January 2003, as required by the USA PATRIOT Act and the Enhanced Border Security and Visa Entry Reform Act, the Attorney General, the Secretary of State, and NIST jointly submitted a report that focuses on specific legislative requirements related to interoperable databases, biometric identifiers, and travel document authentication for entry only.[7] The report discusses the current border control process, the need for a new approach, and identifies several issues that need to be addressed to make a more extensive use of biometrics in automated border control systems.

As a part of this report, NIST developed technical standards for biometric identifiers and tamper-resistance for travel documents. NIST reported that facial recognition and fingerprint recognition are the only biometric technologies with sufficiently large operational databases for testing at this time. NIST concluded that while iris recognition is a promising candidate, it requires collection of a large test database to test the uniqueness of iris data for large samples. NIST recommends that 10 fingerprints be used for background identification, and a dual biometric system using 2 fingerprint images and a face image may be needed to meet projected system requirements for verification. For tamper-resistance, NIST recommended the use of a public key infrastructure to authenticate the source of travel documents. According to the report, the Attorney General and the Secretary of State have agreed to use a live-capture digital photograph and fingerprints for identity enrollment, background checks, and identity verification. However, the exact number of fingerprints required at enrollment has not been finalized.

The report identifies several issues and considerations that need to be further evaluated and resolved. The resolution of these issues will have significant operational, technical, and cost implications. According to the report, if the various stakeholders of this cross-agency effort do not work out these details before major investments are made, the estimated cost and expected results of the investment will be at risk. Further, the report states that due to the size and complexity of the effort, the deployment schedule will need to be delayed at least 1 year from the October 26, 2004, target date established in the legislation.

[7] The Attorney General, Secretary of State, and the National Institute of Standards and Technology, *Report to the Congress: Use of Technology Standards and Interoperable Databases with Machine-Readable, Tamper-Resistant Travel Documents* (Jan. 2003).

Many of the issues identified in the report are consistent with the challenges we identified in our work last year. For example, the report discusses the need to change the end-to-end business process to incorporate the enrollment and verification of biometric information from travelers. Further, the report cites the need to improve border security without a major adverse effect on tourism, commerce, and border traffic flow. Privacy issues and the effect on international relations are also addressed. Exception processing is discussed. According to the report, approximately 2 percent of the population cannot provide good fingerprint images. As a result, an alternate enrollment and identification procedure will be required for these people. To develop the biometric border control system, the report estimates it would cost about $3.8 billion including initial and recurring costs over a six-year period.

The report cites a number of steps that need to be taken by a cross-agency project team to clarify the scope, costs, benefits, and schedule required to implement the legislative requirement. For example, the report cites the need to develop a cross-agency concept of operations for the entire end-to-end process that would guide the scoping, requirements definition, and trade-off analyses required to develop and deploy the system. The concept of operations would also help determine how the proposed solution can balance identity verification and efficient traffic flow objectives at land borders. The report also discusses the need to update the overall costs and benefits of the solution to confirm that the effort will achieve the benefits desired at an acceptable cost. Steps will also need to be taken to align U.S. biometric standards with those of other countries, particularly visa-waiver countries, in a manner consistent with the concept of operations. Finally, the report cites the need to define and establish a cross-agency program management and governance structure to drive the business change and deployment associated with this effort.

Current Inspection Challenges at Land Ports of Entry

As the Department of Homeland Security and other agencies consider a biometrics-based border security concept of operations, they may need to address current challenges that we have observed during our ongoing work at land ports of entry. At a minimum, these challenges represent potential implementation issues that could affect the security benefits intended by the new border security system. These challenges include:

- **Integrity of the Inspections Process.** The need to balance the dual objectives of identifying those who should not be permitted entry into the country and keeping traffic and trade flowing through the ports creates potential weaknesses in the process that biometrics can help

resolve but not entirely. For example, we recently reported on our ability to enter the country at ports of entry with erroneous answers to inspector questions and counterfeit identification. [8] Also, at land ports of entry, computer checks are made on the vehicle that travelers arrive in but not on the driver and passengers unless inspectors suspect wrongdoing. Moreover, we observed that new security procedures aimed at increasing process integrity were not consistently followed. With respect to alternative inspection programs, various trusted traveler programs, intended to process large numbers of pre-screened travelers quickly so that inspectors can devote more time to travelers whose risk is unknown, can be strengthened through wider use of biometrics. Some current programs are not attractive to many travelers because the cost of participation does not ensure time savings when crossing the border.

- **Providing Technology and Equipment to Inspectors.** Some current border operations are time-consuming because inspectors must separately log on and off of several lookout databases that need to be checked when more intensive, or secondary, inspections are required. This could increase the risk that an inspector might overlook valuable information. Further, inspectors still perform many routine administrative processes by hand, although some ports of entry have successfully automated some of these manual processes. Once the concept of operations for a new border security system is adopted, extensive introduction of new equipment and automated processes will require extensive training and reinforcement.

- **Access to Intelligence Information.** The amount of intelligence information border inspectors currently receive in a single day can be overwhelming, and inspectors report that they do not have enough time to read it. Further, because of the need to staff inspection lanes, some ports of entry reported not having time to conduct daily intelligence and safety briefings, as required. Ensuring that intelligence information is relevant, and that inspectors have sufficient time to review and absorb it, will present a significant challenge for a new border security system.

- **Adequate and Consistent Inspector Training.** Merging INS and Customs inspectors into a single shared inspection force will be a significant challenge because INS and Customs train their inspectors at

[8] U.S. General Accounting Office, *Weaknesses In Screening Entrants Into The United States*, GAO-03-438T (Washington D.C.: Jan. 30, 2003).

two separate academies using two different curricula with little time devoted to learning each other's laws and regulations. In addition, training, particularly of new inspectors, is a continuing need after deployment of inspectors, but the pressures of inspection itself has taken precedence over both on-the-job training and formal training at some ports.

In conclusion, biometric technologies are available today that can be used for border security. However, it is important to bear in mind that effective security cannot be achieved by relying on technology alone. Technology and people must work together as part of an overall security process. As we have pointed out, weaknesses in any of these areas, such as those we identified at land ports of entry, diminishes the effectiveness of the security process. We have found that three key considerations need to be addressed before a decision is made to design, develop, and implement biometrics into a border control system:

1. Decisions must be made on how the technology will be used.

2. A detailed cost-benefit analysis must be conducted to determine that the benefits gained from a system outweigh the costs.

3. A trade-off analysis must be conducted between the increased security, which the use of biometrics would provide, and the effect on areas such as privacy and the economy.

A report recently issued jointly by the Attorney General, Secretary of State, and NIST agrees with these considerations. As DHS and other agencies consider the development of a border security system with biometrics, they need to define what the high-level goals of this system will be and develop the concept of operations that will embody the people, process, and technologies required to achieve these goals. With these answers, the proper role of biometric technologies in border security can be determined. If these details are not resolved, the estimated cost and performance of the resulting system will be at risk.

Mr. Chairmen, this concludes my statement. I would be pleased to answer any questions that you or members of the subcommittees may have.

Contacts and Acknowledgments

For further information, please contact Nancy Kingsbury, Managing Director, Applied Research and Methods, at (202) 512-2700, or Richard Stana, Director, Homeland Security and Justice, at (202) 512-8777.
Individuals making key contributions to this testimony include Yvette Banks, Naba Barkakati, Michael Dino, Barbara Guffy, Richard Hung, Rosa Lin, and Lori Weiss.

Related GAO Products

Combating Terrorism: Observations on National Strategies Related to Terrorism. GAO-03-519T. Washington, D.C.: March 3, 2003.

Homeland Security: Challenges Facing the Coast Guard as it Transitions to the New Department. GAO-03-467T. Washington, D.C.: February 12, 2003.

Weaknesses In Screening Entrants Into The United States. GAO-03-438T. Washington, D.C.: January 30, 2003.

Major Management Challenges and Program Risks: Department of Homeland Security. GAO-03-102. Washington, D.C.: January 2003.

Homeland Security: Management Challenges Facing Federal Leadership. GAO-03-260. Washington, D.C.: December 20, 2002.

Homeland Security: Information Technology Funding and Associated Management Issues. GAO-03-250. Washington, D.C.: December 13, 2002.

Border Security: Implications of Eliminating the Visa Waiver Program. GAO-03-38. Washington, D.C.: November 22, 2002.

Homeland Security: INS Cannot Locate Many Aliens Because It Lacks Reliable Address Information. GAO-03-188. Washington, D.C.: November 21, 2002.

Container Security: Current Efforts to Detect Nuclear Materials, New Initiatives, and Challenges. GAO-03-297T. New York, NY: November 18, 2002.

Technology Assessment: Using Biometrics for Border Security. GAO-03-174. Washington, D.C.: November 15, 2002.

Coast Guard: Strategy Needed for Setting and Monitoring Levels of Effort for All Missions. GAO-03-155. Washington, D.C.: November 12, 2002.

Border Security: Visa Process Should Be Strengthened as an Antiterrorism Tool. GAO-03-132NI. Washington, D.C.: October 21, 2002.

Customs Service: Acquisition and Deployment of Radiation Detection Equipment. GAO-03-235T. Washington, D.C.: October 17, 2002.

Homeland Security: Effective Intergovernmental Coordination Is Key to Success. GAO-02-1013T. Washington, D.C.: August 23, 2002.

Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful. GAO-02-993T. Washington, D.C.: August 5, 2002.

Identity Fraud: Prevalence and Links to Alien Illegal Activities. GAO-02-830T. Washington, D.C.: June 25, 2002.

Immigration Enforcement: Challenges to Implementing the INS Interior Enforcement Strategy. GAO-02-861T. Washington, D.C.: June 19, 2002.

National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy. GAO-02-811T. Washington, D.C.: June 7, 2002.

Customs Service Modernization: Management Improvements Needed on High-Risk Automated Commercial Environment Project. GAO-02-545. Washington, D.C.: May 13, 2002.

National Preparedness: Technologies to Secure Federal Buildings. GAO-02-687T. Washington, D.C.: April 25, 2002.

INS Forensic Document Laboratory: Several Factors Impeded Timeliness of Case Processing. GAO-02-410. Washington, D.C.: March 13, 2002.

Immigration Benefit Fraud: Focused Approach Is Needed to Address Problems. GAO-02-66. Washington, D.C.: January 31, 2002.

Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts. GAO-02-208T. Washington, D.C.: October 31, 2001.

Immigration and Naturalization Service: Overview of Recurring Management Challenges. GAO-02-168T. Washington, D.C.: October 17, 2001.

INS Southwest Border Strategy: Resource and Impact Issues Remain After Seven Years. GAO-01-842. Washington, D.C.: August 2, 2001.