Report to Congressional Requesters, House of Representatives

January 2007

# HOMELAND SECURITY

## Progress Has Been Made to Address the Vulnerabilities Exposed by 9/11, but Continued Federal Action Is Needed to Further Mitigate Security Risks

**GAO**

Accountability ★ Integrity ★ Reliability

# HOMELAND SECURITY

# Progress Has Been Made to Address the Vulnerabilities Exposed by 9/11, but Continued Federal Action Is Needed to Further Mitigate Security Risks

## Why GAO Did This Study

Five years after the terrorist attacks of September 11, 2001, GAO is taking stock of key efforts by the President, Congress, federal agencies, and the 9/11 Commission to strengthen or enhance critical layers of defense in aviation and border security that were directly exploited by the 19 terrorist hijackers. Specifically, the report discusses how: (1) commercial aviation security has been enhanced; (2) visa-related policies and programs have evolved to help screen out potential terrorists; (3) federal border security initiatives have evolved to reduce the likelihood of terrorists entering the country through legal checkpoints; and (4) the Department of Homeland Security (DHS) and other agencies are addressing several major post-9/11 strategic challenges.

The report reflects conclusions and recommendations from a body of work issued before and after 9/11 by GAO, the Inspectors General of DHS, State, and Justice, the 9/11 Commission, and others. It is not a comprehensive assessment of all federal initiatives taken or planned in response to 9/11.

GAO is not making any new recommendations at this time since over 75 prior recommendations on aviation security, the Visa Waiver Program, and US-VISIT, among others, are in the process of being implemented. Continued monitoring by GAO will determine whether further recommendations are warranted.

## What GAO Found

While the nation cannot expect to eliminate all risks of terrorist attack upon commercial aviation, agencies have made progress since 9/11 to reduce aviation-related vulnerabilities and enhance the layers of defense directly exploited by the terrorist hijackers. In general, these efforts have resulted in better airline passenger screening procedures designed to identify and prevent known or suspected terrorists, weapons, and explosives from being allowed onto aircraft. Nevertheless, the nation's commercial aviation system remains a highly visible target for terrorism, as evidenced by recent alleged efforts to bring liquid explosives aboard aircraft. DHS and others need to follow through on outstanding congressional requirements and recommendations by GAO and others to enhance security and coordination of passengers and checked baggage, and improve screening procedures for domestic flights, among other needed improvements.

GAO's work indicates that the government has strengthened the *nonimmigrant* visa process as an antiterrorism tool. New measures added rigor to the process by expanding the name-check system used to screen applicants, requiring in-person interviews for nearly all applicants, and revamping consular officials' training to focus on counterterrorism. Nevertheless, the *immigrant* visa process may pose potential security risks and we are reviewing this issue.

To enhance security and screening at legal checkpoints (air, land, and sea ports) at the nation's borders, agencies are using technology to verify foreign travelers' identities and detect fraudulent travel documents such as passports. However, DHS needs to better manage risks posed by the Visa Waiver Program, whereby travelers from 27 countries need not obtain visas for U.S. travel. For example, GAO recommended that DHS require visa-waiver countries to provide information on lost or stolen passports that terrorists could use to gain entry. We also recommended that DHS provide more information to Congress on how it plans to fully implement US-VISIT— a system for tracking the entry, exit, and length of stay of foreign travelers.

While much attention has been focused on mitigating the specific risks of 9/11, other critical assets ranging from passenger rail stations to power plants are also at risk of terrorist attack. Deciding how to address these risks—setting priorities, making trade-offs, allocating resources, and assessing social and economic costs—is essential. Thus, it remains vitally important for DHS to continue to develop and implement a risk-based framework to help target where and how the nation's resources should be invested to strengthen security. The government also faces strategic challenges that potentially affect oversight and execution of new and ongoing homeland security initiatives, and GAO has deemed three challenges in particular—information sharing, risk management, and transforming DHS as a department—as areas needing urgent attention.

DHS and the Department of State reviewed a draft of this report and both agencies generally agreed with the information. Both agencies provided technical comments that were incorporated as appropriate.

**United States Government Accountability Office**

# Contents

**Figures**

**Abbreviations**

| | |
|---|---|
| ATSA | Aviation and Transportation Security Act |
| CBP | Customs and Border Protection |
| DHS | Department of Homeland Security |
| DOT | Department of Transportation |
| EDS | explosive detection systems |
| ETD | explosive trace detection systems |
| FAA | Federal Aviation Administration |
| FRA | Federal Railroad Administration |
| FTA | Federal Transit Administration |
| HSPD | Homeland Security Presidential Directive |
| ICE | Immigration and Customs Enforcement |
| IED | improvised explosive device |
| Interpol | International Criminal Police Organization |
| NORAD | North American Aerospace Defense Command |
| OGT | Office of Grants and Training |
| OIG | Office of Inspector General |
| POE | ports of entry |
| TSA | Transportation Security Administration |
| TSO | transportation security officers |
| TSOC | Transportation Security Operations Center |
| TWIC | Transportation Workers Identification Credential |
| US-VISIT | U.S. Visitor and Immigrant Status Indicator Technology |
| WHTI | Western Hemisphere Travel Initiative |

**GAO**
**Accountability * Integrity * Reliability**

**United States Government Accountability Office**
**Washington, DC 20548**

January 24, 2007

The Honorable Lamar Smith,
Ranking Minority Member
Committee on the Judiciary
House of Representatives

The Honorable F. James Sensenbrenner, Jr.
House of Representatives

The terrorist attacks on September 11, 2001, significantly altered the nation's views on how to secure and protect the people, borders, and assets of the United States, and dramatically highlighted the need to take immediate actions to reduce the likelihood of future attacks of this magnitude taking place on U.S. soil. With the benefit of hindsight, it is apparent that on 9/11, several areas in particular—the U.S. commercial aviation system, the federal government's approach to compiling and managing terrorist watch lists, the nonimmigrant visa process,[1] and mechanisms for screening and recording foreign travelers entering and exiting the United States—were all shown to be vulnerable to exploitation by terrorists intent on gaining entry to the country and wreaking havoc. Clearly, federal action was needed to address these and other weaknesses in our defenses. The federal government simply was not prepared for, and did not anticipate, the ways in which the security measures in place prior to 9/11 would be defeated. As the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) noted in its 2004 report,[2] none of the security measures adopted by the U.S. government prior to the attacks disturbed or even delayed the progress of the al Qaeda plot.

In the 5 years since 19 hijackers commandeered four commercial aircraft and succeeded in destroying the World Trade Center, damaging the

---

[1]A nonimmigrant visa is a U.S. travel document that foreign citizens from many countries must obtain before arriving at U.S. ports of entry to enter the country temporarily for business, tourism, or other reasons. The United States also grants visas to people who intend to immigrate to the United States. In this report, unless otherwise noted, we use the term "visa" to refer to nonimmigrant visas only.

[2]The 9/11 Commission, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, D.C.: July 2004).

Pentagon, and killing almost 3,000 people, Congress and the administration have taken a number of actions to realign homeland security policies, priorities, and resources to help ensure that the 9/11 scenario could never be repeated. To this end, our government has in part reorganized by combining vital federal security, immigration, and investigative capabilities within a new Department of Homeland Security (DHS). Parallel efforts also were undertaken to transform the intelligence community in order to provide better information on, and analysis of, terrorist threats—information that could have serious implications for aviation, the visa process, and the border screening and inspection processes undertaken as part of border security.

Since 9/11, Congress and the administration, including many federal agencies, have increasingly sought to take a longer-term view of homeland security, recognizing, among other things, that a variety of transportation and border security initiatives are needed, such as improving the mechanisms for screening foreign travelers before they enter the country legally by air, land, or sea ports, and tracking their entry and exit. More recent efforts by terrorists to disrupt society—notably, the alleged attempt by terrorists to bring liquid explosives on board aircraft bound for the United States and terrorist attacks on passenger rail systems in Madrid and London—have further highlighted the need for effective information sharing, proactive planning, and effective risk analysis, in order to identify and mitigate risks to people, national assets, and economic sectors and prioritize resources to address them.

In recognition of the fifth anniversary of the 2001 terrorist attacks, you expressed interest in taking stock of some of the efforts by Congress, the administration, and many federal agencies—in concert with state and local governments and the private sector—to identify the nation's security vulnerabilities in key areas and find ways to mitigate them to the fullest extent possible. You asked us to draw upon the growing body of work by us and the Inspectors General that examine many of the key laws, policies, and practices related to homeland security in the post-9/11 period to assess how these security policies and procedures have evolved in response to the actions of the terrorists. While we recognize that it will never be possible to anticipate or mitigate every potential security threat, or to close every gap in our defenses, it is nonetheless important to acknowledge the critical work that has been done to make the country safer—and, looking ahead, to discuss how the government intends to identify, manage, and mitigate risks to domestic security in general, while continuing to protect privacy and the flow of people and commerce. It is also important to review security efforts made to date, in light of Congress'

interest in revisiting the recommendations of the 9/11 Commission, including those addressing aviation and border security challenges, as well as challenges related to sharing homeland security information. The information contained in this report is derived from a security sensitive report that we issued in December 2006 on progress made to address vulnerabilities exposed by 9/11.[3] That report contained detailed information on specific security vulnerabilities.

This report does not undertake a comprehensive assessment of all federal initiatives taken or planned in response to 9/11. Rather, we focus on the progress the nation has made in strengthening or enhancing the critical layers of defense that either were penetrated by the terrorist hijackers of 9/11, or which our work or that of the Inspectors General shows are vulnerable to terrorist exploitation. This critical layered system of defense identifies points of vulnerability wherever they exist, and turns them into targets of opportunity for interdiction. These layers provide a series of independent, overlapping and reinforcing redundancies—domestically, for example, at airports as well as land and sea ports of entry, or outside the country, at consular offices—designed to raise the odds that terrorist activity can be identified and intercepted. This report focuses primarily on three main layers of defense—aviation security, visa security, and border security[4]—and to the extent that our body of work allows, this report also addresses the role that information sharing has played in keeping federal officials and key stakeholders informed as these layers of defense are strengthened.

In particular, this report discusses the following: (1) In what ways has the security of the nation's commercial aviation system been enhanced since 9/11 to reduce the likelihood that terrorists may carry out new attacks using aircraft? (2) How have visa-related policies and programs evolved since 9/11 to help screen out potential terrorists seeking entry into the United States? (3) How have federal border security efforts evolved since 9/11 to reduce the likelihood that terrorists could enter the United States through legal checkpoints? (4) What are the major strategic challenges

---

[3]GAO, *Homeland Security: Progress Has Been Made to Address the Vulnerabilities Exposed by 9/11, but Continued Federal Action is Needed to Further Mitigate Security Risks*, GAO-07-110SU (Washington D.C.: December 2006).

[4]Our discussion of "border security" in this report refers primarily to the border screening and inspection processes undertaken as part of homeland security. It does not include efforts by the U.S. Border Patrol to enforce U.S. immigration law and other federal laws along the 8,000 miles of our international borders with Mexico and Canada and elsewhere.

facing Congress, DHS, and other federal agencies as the post-9/11 era progresses and decisions are made about prioritizing efforts and allocating finite resources to further enhance homeland security?

The overall scope of our review reflects the national layers of defense in place on 9/11, which the terrorists exploited, and other areas with recognized vulnerabilities and security weaknesses where federal actions have been taken and for which we have a body of work. Specifically, the scope of our work encompassed an extensive review of work published by us and others on the conditions leading up to and the actions taken after 9/11 by Congress and federal departments—the departments of Homeland Security, State, and Justice—which now have primary responsibility for establishing and maintaining key layers of national defense (aviation, the visa process, and our borders) exploited by the 9/11 hijackers. To perform our analyses for all the research questions, we reviewed the findings, conclusions, and recommendations from GAO reports, testimonies, and other issued products on security policies and procedures prior to and after 9/11. This review included GAO's work on aviation security, the visa issuance process, and border security initiatives, as well as information on the development and consolidation of federal terrorist watch lists and how this and other sensitive information has been shared among federal agencies, including the Department of Homeland Security, and appropriate state and local personnel, such as law enforcement agencies and private air carriers. We also analyzed our preliminary results from ongoing work related to homeland security that was being conducted at the time of this review (i.e., work that we had under way but had not yet issued) on international aviation passenger prescreening, the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) border security program, and more. In addition to GAO's work, we analyzed reports and testimonies issued after 9/11 by the Inspectors General for the departments of State, Justice, and Homeland Security and the findings of reports and testimonies issued by the 9/11 Commission.

We reviewed key legislation enacted after 9/11, including (but not limited to) the Aviation and Transportation Security Act,[5] the Homeland Security Act of 2002,[6] the Enhanced Border Security and Visa Entry Reform Act of 2002,[7] and the Intelligence Reform and Terrorism Prevention Act of

---

[5]Pub. L. No. 107-71, 115 Stat. 597 (2001).

[6]Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[7]Pub L. No. 107-173, 116 Stat. 543 (2002).

2004;[8] presidential directives, including (but not limited to) Homeland Security Presidential Directive 6 (HSPD-6) on terrorist identification, screening, and tracking and HSPD-7 on critical infrastructure protection responsibilities; and executive orders. In addition to our documentary analysis, we interviewed senior officials at the departments of State and Homeland Security to obtain current information on progress made to implement selected recommendations we had made, and other actions under way by the departments at the time of our review to enhance security in the areas we were addressing—aviation, visa, and border security.

We recognize that there are significant factors that contributed to the terrorists' ability to complete their acts that Congress and the administration have been addressing since 9/11, which we do not discuss in depth in this report. These include vulnerabilities in available intelligence, terrorist financing mechanisms, and the domestic counterterrorism infrastructure in place to address threats within U.S. borders, among others. Nor does our review reflect activities or initiatives not directly related either to strengthening homeland security or to the 9/11 response; thus our review excludes consideration of initiatives aimed at facilitating travel convenience, such as "trusted traveler" programs[9] and implementation of a redress process to remedy the problem associated with passengers misidentified on terrorist watch lists. See appendix III for a list of products issued by GAO and the office of Inspectors General within the departments of Homeland Security, State, and Justice related to the events of 9/11 and homeland security; many of these products are referred to in this report.

Our work was conducted from September 2005 through October 2006 in accordance with generally accepted government auditing standards.

---

[8]Pub. L. No. 108-458, 118 Stat. 3638 (2004).

[9]"Trusted traveler" programs refer to programs under the purview of DHS or U.S. Customs and Border Protection at designated border ports of entry to expedite the processing of pre-approved, international, and low-risk commercial and commuter travelers crossing the borders.

# Results in Brief

On the morning of September 11, 2001, four American jets piloted by terrorists crashed in rapid succession into the north and south towers of the World Trade Center in New York, the western face of the Pentagon in Washington, D.C., and—diverted by passengers away from the U.S. Capitol or the White House—into a field in southern Pennsylvania. In all, nearly 3,000 individuals were killed in the attacks. The events of that morning revealed significant weaknesses in the security of our commercial aviation system, since 19 hijackers had been able to board the aircraft at large commercial airports and threaten crew members and passengers alike with simple weapons they had carried on board—small knives, box cutters, and cans of Mace or pepper spray, and then penetrate the cockpits and take control of the aircraft. At the time, aviation security policies and procedures focused primarily on stopping terrorists who might try to get weapons—such as guns or large knives—past security checkpoints, bring bombs aboard in their checked baggage, or hijack a plane. They did not prepare security personnel or flight crews for terrorists who would use simple weapons to take control of the aircraft and use it as a missile. Though several hijackers were selected prior to boarding to undergo additional screening, this led only to greater scrutiny of their carry-on luggage for large knives or guns and their checked baggage for explosives. Ultimately, all the hijackers were permitted to board.

While the nation cannot expect to eliminate all future risks of terrorist attacks upon commercial aviation, in the 5 years since the attacks of September 11, 2001, progress has been made toward reducing the aviation-related vulnerabilities and enhancing the layers of defense directly exploited by the terrorist hijackers. Nevertheless, federal agencies continue to face the challenge of identifying and addressing the security risks inherent in the nation's commercial aviation system, which plays a vital role in the nation's economy, ferries millions of passengers around the world on a daily basis, and remains a highly visible target for terrorism. DHS and other federal departments are still working to implement congressional requirements and recommendations by us, the 9/11 Commission, and others to address known security weaknesses in commercial aviation and bolster security-related policies and programs already in place. On the positive side, at the direction of the President and the Congress, DHS and other federal departments have taken actions resulting in better airline passenger screening procedures that help to identify and prevent known or suspected terrorists, weapons, and explosives from being allowed onto aircraft. For example, since 9/11, domestic airline passenger prescreening procedures—whereby passengers who may pose a security risk are identified before boarding aircraft—have been enhanced through an identity-matching process that compares prospective passengers' names against an expanded list of terrorist suspects extracted from a consolidated terrorist watch list. This presecreening process has also been enhanced by requiring certain passengers to undergo greater scrutiny prior to boarding. But TSA has not yet met a congressional requirement that it take over responsibility for the passenger identity-matching process from domestic air carriers, in part to improve accuracy in the matching process and to end disclosure of sensitive information on possible terrorists to air carriers. We have recommended that TSA take numerous steps to help meet this requirement and we are monitoring their efforts. Passengers on international flights departing from or traveling to the United States undergo prescreening by DHS's U.S. Customs and Border Protection (CBP). However, this process poses challenges because these flights are allowed to take off before the passenger identity-matching process has been completed by CBP. Such flights therefore remain vulnerable to a terrorist take-over and other risks. CBP is working to address the problem, but a solution has not yet been implemented. We have recently recommended that DHS make key policy and technical decisions necessary to more fully coordinate CBP's international prescreening program with TSA's prospective domestic prescreening program. With respect to passenger checkpoint screening—the physical screening of passengers and their carry-on bags—we have reported that TSA has met

congressional mandates related to deploying its federal aviation security workforce and establishing passenger screening operations at over 400 commercial airports. Moreover, passenger checkpoint screening operations have been enhanced with the aid of technology and more rigorous hands-on screening practices, among other things, in order to aid in detecting prohibited items. But as we have also reported, it is important that TSA continue to invest in and develop technologies for better detecting existing and emerging threats involving explosives. This is especially important in light of the alleged August 2006 plot to detonate liquid explosives on board multiple commercial aircraft bound for the United States from the United Kingdom. DHS and TSA have also taken actions to improve the layers of aviation defense not directly implicated in the 9/11 attacks. For instance, 100 percent of airline passengers' checked baggage is now screened, compared to just a fraction before 9/11, and TSA is seeking more cost-effective ways to deploy baggage screening systems at airports for detecting explosives. It is important to note that in light of the nature of the 9/11 attacks, priority federal attention was initially given to aviation security. Therefore, efforts to improve the security of other transportation modes—without losing sight of ongoing needs in aviation—have not progressed to the same extent. TSA and other federal agencies, including the Department of Transportation and the U.S. Coast Guard, have begun to conduct risk assessments within specific transportation modes, including aviation, passenger rail, maritime, and surface transportation in order to better identify critical assets and to prioritize and allocate finite security resources for protecting these assets. However, as we have reported, these efforts are not complete. DHS and other federal agencies have also recognized the importance of coordinating security-related priorities and activities with domestic and international stakeholders and are taking steps to enhance such cooperation. For example, in response to our recommendation to evaluate foreign passenger rail security practices not currently in use in the United States, TSA is working with foreign counterparts in order to share and glean best practices.

While it is generally acknowledged that the visa process can never be entirely failsafe, the government has done a creditable job overall since 9/11 in strengthening the visa process as a first line of defense to prevent entry into the country by terrorists. Because citizens of other countries seeking to enter the United States on a temporary basis generally must apply for and obtain a nonimmigrant visa, the visa process is important to homeland security. Before 9/11, U.S. visa operations focused primarily on illegal immigration concerns—whether applicants sought to reside and work illegally in the country. Since the attacks, Congress, the State Department, and DHS have implemented several measures to strengthen the entire visa process as a tool to combat terrorism. New policies and programs have since been implemented based, in part, on our recommendations to enhance visa security, improve applicant screening, provide counterterrorism training to consular officials who administer the visa process overseas, and help prevent the fraudulent use of visas for those seeking to gain entry to the country. For example, the number of records available to check the identities of visa applicants against the consolidated terrorist watch list and criminal records was expanded fivefold by the State Department and other agencies between 2001 and 2005. The State Department also has taken steps to mitigate the potential for visa fraud at consular posts by deploying visa fraud investigators to U.S. embassies and consulates and conducting more in-depth analysis of the visa information collected by consulates to identify patterns that may indicate fraud, among other things. (Notably, 2 of the 19 terrorist hijackers on 9/11 used passports that were manipulated in a fraudulent manner to obtain visas.) State Department and DHS officials acknowledge that, while such actions have been beneficial, another type of visa process—specifically, immigrant visas issued to those seeking to reside permanently in the United States—may pose security risks, and we have recently begun a review to identify and analyze these potential security risks.

The ability of potential terrorists to gain entry to or remain in the United States took on added importance after the 9/11 attacks. One individual implicated in but not a direct participant in the 9/11 aviation attacks, convicted terrorist Zacarias Moussaoui—as well as convicted "shoe-bomber" Richard Reid—were permitted, by law, to board flights to the United States with passports, but no visas. Both of these individuals, and millions more, traveled from countries that participate in the Visa Waiver Program whereby citizens of these countries can enter the United States for business or tourism for 90 days or less without first obtaining a visa—this program remains in place today. In addition, three of the 9/11 hijackers were able to over-stay their visas and thus remain in the country long enough to carry out their plan, in part because policies in place before 9/11 did not require agencies to collect data on nonimmigrant visitors in order to track whether they had stayed longer than authorized. And some potential terrorists may be able to enter the country at land border crossings using counterfeit travel documents. Between 2003 and 2006, our undercover investigators were able to successfully enter the United States from Canada and Mexico using fictitious names and counterfeit driver's licenses and birth certificates. These conditions—and the actions taken to exploit them—have heightened awareness that we remain vulnerable to future attacks by individuals who attempt to enter the country at legal checkpoints by taking advantage of diplomatic travel agreements between the United States and other countries, and by using fraudulent or stolen travel documents, including passports, driver's licenses, and birth certificates.

Enhancing security and screening at legal checkpoints at the nation's borders has been and remains a daunting task, and our work and that of others indicates that DHS and other agencies continue to need to identify and address security risks at air, land, and sea ports—critical layers of defense that came under heightened scrutiny after 9/11. One area where security risks remain a challenge is the Visa Waiver Program, which enables citizens from 27 countries to travel to the United States without a visa for business or tourism for 90 days or less. This program carries inherent security, law enforcement, and illegal immigration risks. For example, by design, visa waiver travelers are not subject to the same degree of screening as travelers who must first obtain visas. Convicted 9/11 terrorist Zacarias Moussaoui is among those who carried a passport issued by a visa waiver country. Moreover, lost and stolen passports from visa waiver countries are valuable travel documents for terrorists, criminals, and others who are seeking to hide their true identities to gain entry into the country. Congress, DHS's Office of Inspector General, and we have played a role in DHS's efforts to address these challenges in the context of strengthening border security. Since 2003, DHS has intensified its oversight of visa waiver countries to ensure they comply with the program's statutory requirements, but we have reported that because of staffing challenges, such oversight may not be performed consistently to ensure compliance, and we recently recommended that additional resources be provided for such oversight. To mitigate the misuse of lost or stolen passports—which experts consider the greatest security problem posed by the Visa Waiver Program—DHS provides additional training for CBP officers in fraudulent document detection, and starting on October 26, 2005, passports of visa waiver travelers issued on or after that date, and until October 25, 2006 have to contain a digital photograph as an antifraud measure. Passports issued to visa waiver travelers after October 25, 2006, must be electronic (e-passports). We have recently recommended that DHS take additional steps to mitigate the risks from lost or stolen passports, including requiring all visa waiver countries to provide the United States and Interpol[10] (an international police organization) with data on lost or stolen issued passports as well as blank passports; some visa waiver countries have been reluctant to provide this information. Finding ways to address these and other challenges will be important, given that many countries are actively seeking admission into the program.

---

[10]Interpol is the world's largest international police organization, with 184 member countries. In July 2002, Interpol established a database on lost and stolen travel documents. As of June 2006, the database contained about 11.6 million records of lost and stolen passports.

Separately, a border security initiative known as US-VISIT is intended to serve as a comprehensive system for integrating data on the entry and exit, and verifying the identity, of most foreign travelers coming through the nation's air, land, and sea ports, to mitigate the likelihood that terrorists or criminals can enter or exit at will, or that persons stay longer than authorized. Our work indicates that US-VISIT faces operational and strategic challenges. DHS has made considerable progress installing the entry portion of this system, which allows CBP border officers to verify travelers' identities by, among other things, scanning and comparing digital fingerprints and photographs, and checking biographic information against various federal databases, including the consolidated terrorist watch list. But Congress' goal for US-VISIT—to record the entry, reentry, and exit of travelers, including those who overstay their authorized stay— has not been fully achieved. According to DHS, an exit capability using comparable biometric scanning tools is not yet technologically feasible, would be very costly, and is not likely to be developed or deployed for up to 10 years. Without such a capability, the government cannot provide certainty that persons exiting the country are the same as those entering— and thus cannot determine which visitors have overstayed their authorized stay. We recently recommended that, among other things, DHS should finalize a mandated report to Congress describing how a comprehensive biometrically based entry and exit system would work in order to achieve US-VISIT's intended goals. Agencies need to address other border-related vulnerabilities as well. For example, CBP, along with the departments of Energy, Defense, and State, have taken steps to combat the smuggling of hazardous materials and cargo at ports of entry through use of better radiation detection equipment and inter-agency coordination, among other things. But our undercover investigators were nonetheless able within the last year to purchase and bring radioactive material across the border due to weaknesses in federal regulations governing the suppliers of such materials and the failure of CBP officers to detect counterfeit documentation presented during the border inspection process. In response to our work, officials with the Nuclear Regulatory Commission told us that they are aware of the potential problems with counterfeit documentation and are working to resolve these issues. While it may never be possible to ensure that terrorists, criminals, or those violating immigration laws are prevented from entering the country, DHS and other agencies must remain vigilant in developing and implementing programs and policies designed to reduce breaches in national borders and ensure that potential terrorists, as well as hazardous cargo, are interdicted.

The aviation and border security vulnerabilities exploited by the 9/11 terrorists—and terrorist threats that have come to light since—underscore

the need for continued vigilance and for ensuring that federal agencies, the private sector, and other stakeholders coordinate their efforts, and deploy their resources, as strategically and cost effectively as possible. While much has been accomplished to mitigate specific risks from terrorism, Congress, DHS, and other federal agencies nevertheless continue to face an array of strategic challenges that potentially affect oversight and execution of the efforts that are under way or planned to enhance homeland security in the wake of 9/11 and new terrorist threats. Choosing an appropriate course of action going forward—setting priorities and making trade-offs, allocating resources, and assessing the social and economic costs of the measures that may be taken governmentwide—is not easy, but is nonetheless essential. One of the most important of these strategic challenges involves improving the sharing of information related to terrorism—a major acknowledged weakness at the time of 9/11. As a member of the 9/11 Commission noted, for example, information collected about terrorist suspects by the CIA and FBI at the time of the attacks was not shared with the Federal Aviation Administration (FAA). We designated information sharing for homeland security as a governmentwide high-risk area in 2005—meaning an area that needs urgent attention and transformation to ensure that our national government functions in the most economical, efficient, and effective manner possible. Responding to the lessons of 9/11, Congress and federal departments have taken steps to improve information sharing across the federal government and in conjunction with state and local governments and law enforcement agencies. For example, as we have reported, a consolidated terrorism watch list has been created and more broadly shared among key federal agencies to provide information that can be used to identify terrorists traveling to and within the United States. In addition, the FBI has increased its field-based joint terrorism task forces that bring together personnel from all levels of government to combat terrorism by sharing information and resources. And DHS has implemented homeland security information networks to share relevant information with states and localities. But the government continues to face significant information-sharing challenges. For example, Congress has required establishing an information sharing environment that would combine policies, procedures, and technologies that link people, systems, and information among all appropriate federal, state, local, and tribal entities and the private sector. We have recommended that in planning for this environment, responsible officials identify and address barriers posed by resource needs, among other things.

A second strategic challenge facing the nation involves the application of a risk management framework that requires, at the highest level, the

balancing of security concerns against other needs, given finite resource levels. Such a framework is needed as a way to consider how much the nation can afford to spend for security improvements in light of other, competing demands for limited funds, such as increasing costs of health care, Social Security, and other domestic problems. In our January 2005 report on high-risk areas in the federal government, we noted the importance of completing comprehensive national threat and risk assessments to guide and prioritize investment decisions—and noted risk management as an emerging area of concern. Much is also at stake when decisions are made about how to allocate limited resources across a large number of programs in multiple agencies. DHS is still in the early stages of adopting a risk-based strategic framework for making important resource decisions involving billions of dollars annually. In part, this is because the process is difficult and complex; requires comprehensive information on risks and vulnerabilities; and employs sophisticated assessment methodologies. The process also requires careful trade-offs that balance security concerns against other needs. With its fiscal year 2007 budget of about $35 billion, DHS has begun conducting risk assessments at individual infrastructure facilities and allocating grants based on risk criteria. But the agency has not completed all of the necessary risk assessments mandated by the Homeland Security Act to set priorities to help focus its resources where most needed. We have made numerous recommendations in these areas, which DHS is in the process of implementing.

Finally, DHS faces significant management and organizational transformation challenges as it works to protect the nation from terrorism and implement effective risk management policies. As we have noted, DHS must continue to integrate approximately 180,000 employees from 22 originating agencies, consolidate multiple management systems and processes, and transform into a more effective organization with robust planning, management, and operations. For these reasons, we continue to designate the implementation and transformation of the department as high risk (meaning an area requiring urgent attention), and will continue to monitor and report on its progress. While national needs to reduce vulnerabilities suggest a rapid organization of homeland security functions, we recognize that such dramatic transitions of agencies and programs, as well as the breadth and scope of management support functions that need to be incorporated into the new department, are likely to take time to achieve. We should not expect this effort to be easy or the path forward to be smooth. These activities will require sustained management commitment—and continued involvement, support, and oversight by Congress.

Because DHS and other federal agencies are continuing to improve their processes and practices based on many past recommendations by us, the Inspectors General, and others, we are not making new recommendations in this report. For example, we have made over 75 recommendations on aviation security, including actions to enhance the security and improve coordination of airline passenger and checked baggage screening procedures for domestic flights; the Visa Waiver Program, including actions to improve program oversight and mitigate program risks through additional resources and enhanced inter-governmental cooperation; and border screening and inspection processes, including actions need to complete the US-VISIT entry and exit system for foreign travelers, and more. Continued monitoring of these and related areas by us will determine whether further recommendations are warranted.

We provided DHS and State with a draft of this report for review and comment. Both agencies generally agreed with the information in the report, and both provided technical comments, which we incorporated as appropriate. In addition, DHS provided clarification in two areas. In response to our assertion that the department has not completed all of the necessary risk assessments mandated by the Homeland Security Act of 2002, DHS stated that the act did not specify how many of such assessments were to be completed. DHS also noted that it believes it has made considerable progress by working on vulnerability assessment methodologies across different economic sectors and by providing tools to public and private sector partners to help identify and mitigate vulnerabilities that had been identified. In response to our reference to a DHS Office of Inspector General report that found that DHS had not yet created a comprehensive national inventory of critical infrastructure assets, DHS stated that it remains committed to developing this tool as an evolving, comprehensive catalog of assets that comprise the nation's infrastructure and that support risk analysis. DHS's comments appear in appendix IV. The State Department did not provide formal written comments.

# Background

## Overview of Key Legislation Enacted After 9/11 Related to Aviation and Border Security

After the attacks of September 11, 2001, Congress and the President enacted several new laws intended to address many of the vulnerabilities exploited by the terrorists by strengthening layers of defense related to aviation and border security. A summary of key legislative efforts follows.

To strengthen transportation security, the Aviation and Transportation Security Act (ATSA)[11] was signed into law on November 19, 2001, with the primary goal of strengthening the security of the nation's aviation system. To this end, ATSA created the Transportation Security Administration (TSA) as an agency within the Department of Transportation (DOT) with responsibility for securing all modes of transportation, including aviation.[12] ATSA included numerous requirements with deadlines for TSA to implement that were designed to strengthen the various aviation layers of defense. For example, ATSA required TSA to create a federal workforce to assume the job of conducting passenger and checked baggage screening from air carriers at commercial airports.[13] The act also gave TSA regulatory authority over all transportation modes.

After ATSA was enacted, the Homeland Security Act of 2002 consolidated most federal agencies charged with providing homeland security, including securing our nation's borders, into the newly formed Department of Homeland Security (DHS), which was created to improve, among other things, coordination, communication, and information sharing among the multiple federal agencies responsible for protecting the homeland.

Legislation also was enacted to enhance various aspects of border security. The Homeland Security Act, for example, generally grants DHS exclusive authority to issue regulations on, administer, and enforce the Immigration and Nationality Act and all other immigration and nationality laws relating to the functions of U.S. consular officers in connection with the granting or denial of visas. The Homeland Security Act authorized DHS, among other things, to assign employees to U.S. embassies and consulates to provide expert advice and training to consular officers regarding specific threats related to the visa process.[14]

---

[11]Pub. L. No. 107-71, 115 Stat. 597 (2001).

[12] The Homeland Security Act of 2002, signed into law on Nov. 25, 2002, transferred TSA from the DOT to the new Department of Homeland Security. Pub. L. No. 107-296, § 403, 116 Stat. 2135, 2178.

[13]Prior to the passage of ATSA, the screening of passengers and checked baggage had been performed by private companies under contract to the airlines. The Federal Aviation Administration (FAA) was responsible for ensuring compliance with screening regulations.

[14]The Department of State consular officers overseas maintain responsibility for the visa process and consular officials are part of State, not DHS.

New legislation also was enacted that contained provisions affecting a major border security initiative that had begun prior to 9/11—a system for integrating data on the entry and exit of certain foreign nationals into and out of the United States, now known as US-VISIT (U.S. Visitor and Immigrant Status Indicator Technology). In 2001, the USA PATRIOT Act provided that, in developing this integrated entry and exit data system, the Attorney General (now Secretary of Homeland Security) and Secretary of State were to focus particularly on the utilization of biometric technology (such as digital fingerprints) and the development of tamper-resistant documents readable at ports of entry (either a land, air, or sea border crossing associated with inspection and admission of certain foreign nationals).[15] 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. In addition, the Enhanced Border Security and Visa Entry Reform Act of 2002[16] required that, in developing the integrated entry and exit data system for ports of entry, the Attorney General (now Secretary of Homeland Security) and Secretary of State implement, fund, and use the technology standard that was required to be developed under the USA PATRIOT Act at U.S. ports of entry and at consular posts abroad. The act also required the establishment of a database containing the arrival and departure data from machine-readable visas, passports, and other travel and entry documents possessed by aliens and the interoperability of all security databases relevant to making determinations of admissibility under section 212 of the Immigration and Nationality Act. (For additional information on legislative requirements related to US-VISIT, see GAO, *Border Security: US-VISIT Faces Strategic, Technological, and Operational Challenges at Land Ports of Entry*, GAO-07-248 [Washington, D.C.: December 2006]).

In December 2004, the Intelligence Reform and Terrorism Prevention Act of 2004[17] was enacted, containing provisions designed to address many of the transportation and border security vulnerabilities identified, and recommendations made by the 9/11 Commission. It included provisions designed to strengthen aviation security, information sharing, visa issuance, border security, and other areas. For example, the act mandated

---

[15]Pub. L. No. 107-56, 115 Stat. 272 (2001).

[16]Pub. L. No. 107-173 116 Stat. 543 (2002).

[17]Pub. L. No. 108-458, 118 Stat. 3638.

that TSA develop a passenger prescreening system that would compare passenger information for domestic flights to government watch list information, a function that was at the time, and still is, being performed by air carriers. The act also required the development of risk-based priorities across all transportation modes and a strategic plan describing roles and missions related to transportation security for encouraging private sector cooperation and participation in the implementation of such a plan. In addition, the act required DHS to develop and submit to Congress a plan for full implementation of US-VISIT as an automated biometric entry and exit data system and required the collection of biometric exit data for all individuals required to provide biometric entry data.

## Overview of Key Presidential Policy Directives Issued After 9/11 Related to Aviation and Border Security

In an effort to increase homeland security following the terrorist attacks on the United States, President Bush issued the National Strategy for Homeland Security in July 2002. The strategy sets forth overall objectives to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, minimize the damage and assist in the recovery from attacks that may occur. The strategy is organized into six critical mission areas, including (for purposes of this report) one on border and transportation security. For this mission area, in particular, the strategy specified several objectives, including ensuring the integrity of our borders and preventing the entry of unwanted persons into our country. To accomplish this, the strategy provides for, among other things, reform of immigration services, large-scale modernization of border crossings, and consolidation of federal watch lists. It also acknowledges that accomplishing these goals will require overhauling the border security process.

The President has also issued 16 homeland security presidential directives (HSPD), in addition to the strategy that was issued in 2002, providing additional guidance related to the mission areas outlined in the National Strategy. For example, HSPD-6 sets forth policy related to the consolidation of the government's approach to terrorism screening and provides for the appropriate and lawful use of terrorist information in screening processes. HSPD-11 builds upon this directive by setting forth the nation's policy with regard to comprehensive terrorist-related screening procedures through detecting, identifying, tracking, and interdicting people and cargo that pose a threat to homeland security, among other things. Additionally, HSPD-7 establishes a national policy for federal departments and agencies to identify and prioritize critical infrastructure and key resources and to protect them from terrorist

attacks. (For additional information on the National Strategy for Homeland Security and related presidential directives, see GAO, *Homeland Security: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security,* GAO-05-33 [Washington, D.C.: January 2005]).

## Overview of Key Federal Security-Related Roles and Responsibilities in Post-9/11 Era

The federal departments with primary security-related responsibilities for aviation and border security after 9/11—the frontline departments providing key layers of defense—which are included in this report are shown in figure 1.

**Figure 1: Selected Federal Departments and Agencies with Security Responsibilities**
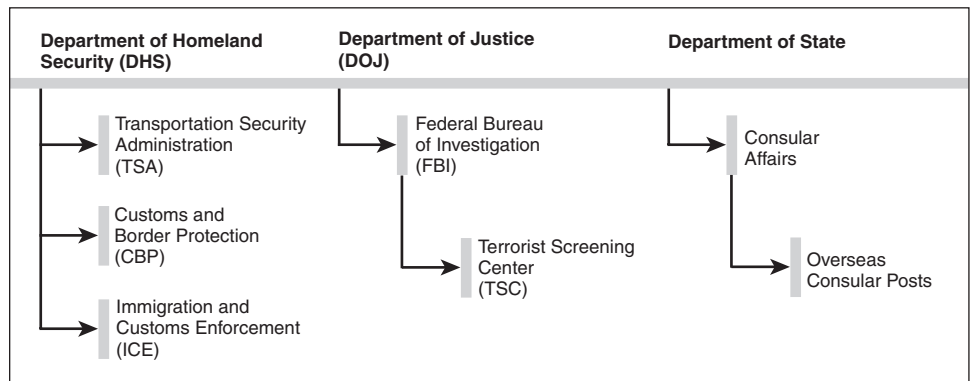


Source: GAO.

## Aviation Security: TSA Has Operational Responsibility for Passenger and Baggage Screening, and Regulatory Responsibility for Air Cargo and Airport Security

The terrorist attacks of September 11, 2001, became the impetus for change in both the way in which airline passengers are screened and the entities responsible for conducting the screening. With the passage of ATSA, TSA assumed responsibility for civil aviation security from the Federal Aviation Administration (FAA), and for passenger and baggage screening from the air carriers.[18] As part of this responsibility, TSA oversees security operations at the nation's more than 400 commercial airports, including passenger and checked baggage screening operations. One of the most significant changes mandated by ATSA was the shift from the use of private-sector screeners to perform airport screening operations to the use of federal screeners. Prior to ATSA, passenger and checked

---

[18]Prior to the passage of ATSA, the screening of passengers and checked baggage had been performed by private companies under contract to the airlines. The Federal Aviation Administration was responsible for ensuring compliance with screening regulations.

baggage screening had been performed by private screening companies under contract to airlines. ATSA required TSA to create a federal workforce to assume the job of conducting passenger and checked baggage screening at commercial airports. The federal workforce was in place, as required, by November 2002. While TSA took over responsibility for passenger checkpoint and baggage screening, air carriers have continued to conduct passenger prescreening (the process of checking passengers' names against federal watch list data at the time after an airline reservation is made). As noted above, the Intelligence Reform and Terrorism Prevention Act requires that TSA take over this responsibility from air carriers.

In addition to establishing requirements for passenger and checked baggage screening, ATSA charged TSA with the responsibility for ensuring the security of air cargo. TSA's responsibilities include, among other things, establishing security rules and regulations covering domestic and foreign passenger carriers that transport cargo, domestic and foreign all-cargo carriers, and domestic indirect air carriers—carriers that consolidate air cargo from multiple shippers and deliver it to air carriers to be transported; and overseeing implementation of air cargo security requirements by air carriers and indirect air carriers through compliance inspections. In general, TSA inspections are designed to ensure air carrier compliance with air cargo security requirements, while air carrier inspections focus on ensuring that cargo does not contain weapons, explosives, or stowaways.

ATSA also granted TSA the responsibility for overseeing U.S. airport operators' efforts to maintain and improve the security of airport perimeters, the adequacy of controls restricting unauthorized access to secured areas, and security measures pertaining to individuals who work at airports. While airport operators, not TSA, have direct day-to-day operational responsibilities for these areas of security, ATSA directs TSA to improve the security of airport perimeters and the access controls leading to secured airport areas, as well as take measures to reduce the security risks posed by airport workers.

**Border Security: State Department and DHS's Customs and Border Protection Have Primary Responsibility for Visa Management and Border Inspection**

Our nation's current border security process is intended to control the entry and exit of foreign nationals seeking to enter or remain in the United States as well as prevent hazardous cargo or materials from being transported into the country. The primary federal agencies involved in this effort are the Department of State's Bureau of Consular Affairs and DHS's Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE).

**Managing and Administering the Visa Process**

The first layer of border security begins at the State Department's overseas consular posts, where State's consular officers are to adjudicate visa applications for foreign nationals who wish to enter the United States. In deciding to approve or deny a visa, consular officers are on the front line of defense in protecting the United States against potential terrorists and others whose entry would likely be harmful to U.S. national interests. Consular officers must balance this security responsibility against the need to facilitate legitimate travel. The process for determining who will be issued or refused a visa contains several steps, including documentation reviews, in-person interviews, collection of biometrics (fingerprints), and cross-referencing an applicant's name against a name-check database that includes the names of visa applicants to identify terrorists and other aliens who are potentially ineligible for visas based on criminal histories or other reasons specified by federal statute. In addition, State provides guidance, in consultation with DHS, to consular officers regarding visa policies and procedures and has the lead role with respect to foreign policy-related visa issues. While State manages the visa process, DHS is responsible for establishing visa policy, reviewing implementation of the policy, and providing additional direction. In addition, DHS had designated ICE to oversee efforts to review applications and provide expert advice and training to consular officers regarding specific threats related to the visa process at certain overseas posts.

**Border Screening and Inspection Processes for Ports of Entry**

CBP is responsible for conducting immigration and customs inspections for aliens entering the United States at official border crossings (air, land, and sea ports of entry). CBP enforces immigration laws by screening and inspecting international travelers who enter the country through ports of entry. As part of this process, CBP officers verify travelers' identities through inspection of travel documents, screen travelers against terrorist watch lists, and scan or enter passport data into databases to verify travelers' identities. CBP also is responsible for conducting customs-related inspections of cargo at ports of entry and for ensuring that all goods entering the United States do so legally. In addition, CBP conducts prescreening of passengers on international flights bound for or departing from the United States. Specifically, CBP reviews biographical data and passport numbers provided by air carriers and conducts queries against terrorist watch lists and law enforcement and immigration databases to determine whether any passengers are to be referred to secondary inspection (whereby passengers are selected for more in-depth review of

GAO-07-375  Progress to Address Security After 9/11

their identity and documentation) prior to the arrival of the aircraft at a U.S. port of entry.

## Federal Use of the Terrorist Watch List to Enhance Aviation and Border Security

The consolidated terrorist watch list is an important tool used by federal agencies to help secure our nation's borders. This list provides decision makers with information about individuals who are known or suspected terrorists, so that these individuals can either be prevented from entering the country, apprehended while in the country, or apprehended as they attempt to exit the country. After 9/11, various government watch lists were consolidated into one watch list, which is maintained by the FBI's Terrorist Screening Center (an entity that has been operational since December 2003 under the administration of the FBI).[19] The consolidated watch list maintained by the center is the U.S. government's master repository for all known and suspected international and domestic terrorist records used for watch list-related screening. The consolidated watch list is an important homeland security tool used by federal frontline screening agencies, including the departments of State, Justice, and Homeland Security. Based upon agency-specific policies and criteria, relevant portions of the consolidated watch list can be used in a wide range of security-related screening procedures. For instance, air carriers and CBP use subsets of the consolidated watch list to prescreen passengers; State Department consular officers use the information in the visa application process; CBP officers use watch list data as part of the visitor inspection process at ports of entry, and state and local law enforcement officers use watch list data to screen apprehended individuals during traffic stops and for other purposes.

## Assessing and Managing Homeland Security Risks Using a Risk Management Approach

In recent years, we, along with Congress (most recently through the Intelligence Reform and Terrorism Prevention Act of 2004); the executive branch (e.g., in presidential directives); and the 9/11 Commission have required or advocated that federal agencies with homeland security responsibilities utilize a risk management approach to help ensure that finite national resources are dedicated to assets or activities considered to

---

[19]Pursuant to Homeland Security Presidential Directive 6, dated Sept. 16, 2003, the FBI's Terrorist Screening Center was established to consolidate the government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes. The center began "24/7" operations on Dec. 1, 2003, and about 3 months later, announced that watch list consolidation was completed on Mar. 12, 2004—with the establishment of the terrorist screening database.

have the highest security priority. We have concluded that without a risk management approach, there is limited assurance that programs designed to combat terrorism are properly prioritized and focused. Thus, risk management, as applied in the homeland security context, can help to more effectively and efficiently prepare defenses against acts of terrorism and other threats. A risk management approach entails a continuous process of managing risk through a series of actions, including setting strategic goals and objectives, performing risk assessments, evaluating alternative actions to reduce identified risks by preventing or mitigating their impact, selecting actions to undertake by management, and implementing and monitoring those actions.

# Stronger Layered Defenses for Aviation Security in Place, Though We Reported More Needs to Be Done to Enhance Passenger Screening Operations and Security of Other Transportation Modes

TSA and other agencies have taken steps to strengthen the various layers of commercial aviation defense—including passenger prescreening (conducted after a reservation is made), passenger checkpoint screening (conducted once passengers are at the airport and proceeding to the gate with any carry-on bags), and in-flight security—that were exploited by the hijackers on 9/11. Many of the vulnerabilities related to these areas have been addressed through new legislation passed by Congress and policies and procedures taken by various federal agencies, though opportunities exist for additional improvements. For example, passengers selected for additional screening after they make their airline reservations receive greater scrutiny prior to boarding, but we have reported that more work is needed to help ensure the process for identifying passengers who are selected results in accurate identification, and TSA has yet to take full responsibility for this process, as mandated. In other areas, passenger checkpoint screening procedures and technologies have been enhanced to aid in detecting prohibited items, and security measures for preparing or responding to in-flight on-board threats, and coordinating responses from the ground, have been strengthened. In addition, other layers of defense in our aviation system have been strengthened, such as checked baggage and air cargo screening, though challenges remain. In baggage screening, for example, while TSA now screens 100 percent of checked baggage using explosive detection systems, enhancing the effectiveness of current baggage screening technologies—and finding the most cost-effective approaches for deploying baggage screening systems to detect explosives—remains challenging. Finally, because we cannot afford to protect everything against all threats in the post-9/11 era, choices must be made about targeting security priorities. Thus, great care needs to be taken to assign available resources to address the greatest risks, along with selecting those strategies that make the most efficient and effective use of resources—within aviation as well as among other transportation

## While Many of the Aviation Vulnerabilities of 9/11 Have Been Addressed, TSA and Other Agencies Continue Efforts to Further Strengthen Aviation Security

security modes, such as passenger rail and maritime industries. TSA and other federal agencies have begun focusing on identifying and prioritizing security needs in these and other areas using a risk-based approach to guide security-related decision making. In addition, efforts are under way to enhance cooperation with domestic and international partners on a broad array of security concerns.

At the time of the 9/11 attacks, federal and airline industry rules for commercial airline travel reflected a system that sought to balance security concerns with the need to facilitate consumer travel and manage growing demand. The events of that day revealed many ways in which more stringent security measures were needed for a commercial aviation system that was evidently vulnerable to terrorism. In particular, the nation's layered system of defense for aviation—including passenger prescreening, passenger checkpoint screening, and in-flight security measures—were not designed to stop the terrorist hijackers from boarding and taking control of the aircraft. A review of aviation security conditions in place prior to 9/11, and the many federal actions taken since then to mitigate the known vulnerabilities, suggest that we have come a long way toward making air travel safer. That said, our work, and that of others, has identified additional actions that are needed to resolve strategic and operational barriers to further enhance the layers of defense for the nation's aviation system.

### Domestic Airline Passenger Prescreening Procedures Have Been Enhanced but We Have Reported That More Work Is Needed to Help Ensure Accuracy in Matching Passengers' Identities against Terrorist Watch Lists

The prescreening of passengers—the process of identifying passengers who may pose a security risk before they board an aircraft—is an important first layer of defense that is intended to help officials focus security efforts on those passengers representing the greatest potential threat. At the time of the attacks, the passenger prescreening process was made up of two components performed by air carriers in conjunction with FAA: (1) a process to compare passenger names with names on a government-supplied terrorist watch list (i.e., the identity-matching process); and (2) a computer-assisted prescreening system that was used to select passengers requiring additional scrutiny. With respect to the first of these passenger prescreening components, after passengers made their airline reservations, the air carriers used the information passengers had provided (such as name and address) to check them against a no-fly list—a government watch list of persons who were considered by the FBI to be a direct threat to U.S. civil aviation, and which was distributed to the U.S. air carriers by FAA. None of the 19 hijackers who purchased their airline tickets for the four 9/11 flights in a short period at the end of August 2001 using credit cards, debit cards, or cash, was on the no-fly list. This list

contained the names of just 12 terrorist suspects; the information for the no-fly list came from one source, the FBI. Other government lists in place at the time contained the names of many thousands of known and suspected terrorists—but were not used to prescreen airline passengers.

In the aftermath of the terrorist attacks, the federal government recognized that effective prescreening of airline passengers largely depended on obtaining accurate, reliable, and timely information on potential terrorists and gave priority attention to, among other things, developing more comprehensive and consolidated terrorist watch lists. In response, in part, to recommendations by us,[20] government watch lists were subsequently consolidated into a terrorist screening database—also known as the consolidated watch list—maintained by the FBI's Terrorist Screening Center.[21] The consolidated watch list maintained by the center is the U.S. government's master repository for all known and suspected international and domestic terrorist records used for watch list-related screening. This watch list database contains records from several sources, including the FBI's list of terrorist organizations and information from the intelligence community on the identity of any known terrorists with international ties.[22] For aviation security purposes, a portion of this consolidated watch list is exported by the Terrorist Screening Center and incorporated into TSA's no-fly and selectee lists.[23] (While according to TSA, persons on the no-fly list should be precluded from boarding an aircraft bound for, or departing from, the United States, any person on the

---

[20]In April 2003, we reported that terrorist and criminal watch lists were maintained by numerous federal agencies and that the agencies did not have a consistent and uniform approach to sharing information on individuals with possible links to terrorism [GAO, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, GAO-03-322 (Washington, D.C.: Apr. 15, 2003)]. Our report recommended that DHS lead an effort to consolidate and standardize the federal government's watch list structures and policies.

[21]Pursuant to Homeland Security Presidential Directive 6, dated Sept. 16, 2003, the FBI's Terrorist Screening Center was established to consolidate the government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes. The center began "24/7" operations on Dec. 1, 2003, and about 3 months later, announced that watch list consolidation was completed on Mar. 12, 2004—with the establishment of the terrorist screening database.

[22]The number of records contained in the watch list database is sensitive security information.

[23]FAA assumed administration of the no-fly list from the FBI in November, 2001. The no-fly list was subsequently split into the no-fly and selectee list when TSA took over administration of the list.

selectee list is to receive additional screening before being allowed to board.) TSA provides updated lists to air carriers for use in prescreening passengers and provides assistance to air carriers in determining whether passengers are a match with persons on the lists. As of June 2006, the number of records in the consolidated watch list that had been extracted for the no-fly and selectee lists had been increased significantly (up from 12 records available on 9/11).[24]

With respect to the second component of passenger prescreening, a computer-assisted prescreening system was in place on 9/11, in which data related to a passenger's reservation and travel itinerary were compared by the air carriers against behavioral characteristics used to identify passengers who appeared to pose a higher than normal risk, and who therefore would be selected for additional security attention prior to their flights.[25] While nine of the 9/11 terrorists were selected for additional scrutiny by the air carriers' computer-assisted prescreening process, there was little consequence to their selection because, at the time, selection only entailed having one's checked baggage screened for explosives or held off the airplane until one had boarded; it was not geared toward identifying the weapons and tactics used by the hijackers.[26] The consequences of selection reflected the view that non-suicide bombing was the most substantial risk to domestic aircraft and were designed to identify individuals who might try to bomb a passenger jet using methods similar to those employed in the 1988 bombing of Pan Am Flight 103 over Lockerbie, Scotland, in which a bomb was placed in checked luggage.

After the passage of ATSA in November 2001, which created TSA as the agency responsible for ensuring the security of aviation and other transportation modes, TSA took over responsibility for the secondary screening process from the air carriers. TSA subsequently changed the consequences for passengers selected by the prescreening process. Currently, passengers who are selected for secondary prescreening either

---

[24]The number of records contained in the no-fly and selectee lists is sensitive security information.

[25]At the time of 9/11 attacks, individuals who could not produce an approved form of identification as well as those unable to answer standard security questions asked by air carrier employees, such as, "Did you pack your own bags?", would also receive additional screening.

[26]Three of the nine hijackers selected had their checked bags scanned for explosives before being loaded on the plane. Five of the nine hijackers selected had their checked bags held until they had boarded the aircraft. The remaining hijacker did not check any bags.

because they are on TSA's selectee list or because they are selected by an air carrier's computer-assisted passenger prescreening system now receive more comprehensive secondary screening. Specifically, all these selectees not only receive greater passenger-checked baggage screening than nonselectees, as was the case at the time of terrorist attacks, but also receive additional physical screening, such as a hand-search of their luggage and a more thorough physical inspection of their person at the checkpoint.

All of these efforts have helped to transform the prescreening process into a more robust layer of defense than existed prior to 9/11. Nevertheless, the federal government still faces challenges related to improving the identity-matching portion of the prescreening process to help ensure that known or suspected terrorists are identified before they can board aircraft. For example, while the process of developing and maintaining terrorist watch lists to be used in the identity-matching process requires continuous effort, and no watch list can ever promise to contain a match for every potential traveler, ensuring the quality of watch list data nevertheless remains a key challenge. Concerns have been raised about the overall quality of the consolidated watch list—in particular, that the quality of data in the watch lists varies, and that the underlying accuracy of the data in the consolidated watch list has not been fully determined. The Department of Justice Inspector General reported in June 2005[27] that the Terrorist Screening Center could not ensure the information in the consolidated watch list database maintained by the center was complete and accurate. For example, the database did not contain names that should be included in watch lists, according to the Inspector General, and it contained inaccurate information about some persons who were on the lists. According to the Inspector General's report, the Terrorist Screening Center is working on completing a record-by-record quality assurance review of the watch lists to ensure that each record contains the required data to improve watch list quality. In addition, screening center officials have recently stated that all records on the no-fly list are being re-vetted using newly developed no-fly list inclusion guidance to determine if each individual truly belongs on the list. We have work under way addressing the law enforcement response agencies take when an individual on the watch list is encountered.

---

[27]U.S. Department of Justice Office of the Inspector General, *Review of the Terrorist Screening Center*, Audit Report 05-27 (June 2005).

A second challenge that affects the accuracy of the current identity-matching process relates to the nature of the information available to air carriers and the procedures used to match passenger identities against the no-fly and selectee lists that are part of the consolidated terrorist watch list. Although air carriers are required to compare the information supplied by passengers against the names that appear on the no-fly and selectee lists, there is no uniform identity matching process or common software that all air carriers are required to use to conduct their identity matching procedures. In addition, the technical sophistication of air carrier identity matching techniques also varies. Some identity matching technologies might correctly discriminate between "John Smith" and "John Smythe" when comparing these names against the consolidated terrorist watch list, while others may not. Different identity matching results can lead to a passenger being boarded on one carrier's flight while being denied boarding on another air carrier's flight, including a connecting flight. Although we did not assess the relative accuracy of the various name-matching procedures used to prescreen passengers, inconsistency in these procedures can be problematic for passengers and creates security concerns.[28]

A third challenge relates to concerns about the disclosure of watch list information outside the federal government. Sharing of watch list data with air carriers, or organizations with whom they contract, creates an opportunity for watch lists to be viewed by parties who may use this information in ways that are detrimental to U.S. interests. For example, if a terrorist group could view the no-fly and selectee lists they would learn which—if any—of their operatives would be able to travel on commercial aircraft to or from the United States unhampered. In addition, the 9/11 Commission stated that there are security concerns with sharing U.S. government watch lists with private firms and foreign countries.[29]

In an effort to address these security challenges, the commission recommended that TSA take over the domestic watch list identify-

---

[28]We have ongoing work assessing air carriers' current identity matching procedures for prescreening passengers on domestic flights.

[29]The 9/11 Commission noted that under current practices, air carriers enforce government orders to stop certain known and suspected terrorists from boarding commercial flights and to apply secondary screening procedures to others. Because air carriers implement this prescreening program, concerns about sharing intelligence with private firms and foreign countries keep the U.S. government from listing all terrorist and terrorist suspects who should be included in the watch lists.

matching process from air carriers, and in December 2004, Congress required that the responsibility for the domestic watch list identity-matching process be assumed by TSA.[30] While shifting control over the watch list identity-matching process from the airline industry to the federal government should help address some of the limitations of the current process, for over 3 years, TSA has faced significant challenges in developing and implementing a new and more reliable identity-matching process, and has not yet taken this function over from air carriers. TSA's Secure Flight[31] program—which is to perform the functions associated with determining whether passengers on domestic flights are on government watch lists—is intended to remedy some of the problems in the current identity-matching process. For example, unlike the current system that operates as part of each air carrier's reservation system, Secure Flight would be operated by TSA—and TSA, rather than the air carriers, would be responsible for matching passengers' names against the no-fly and selectee information maintained in the consolidated watch list (this information is currently transmitted to air carriers) as well as information from other watch lists. This approach would, among other benefits, eliminate the need to distribute terrorist watch list information outside the federal government as part of passenger prescreening. In addition, Secure Flight is intended to address the problem related to the lack of standard procedures among air carriers for obtaining passenger-supplied data by defining what type of passenger information is required. Secure Flight also plans, among other things, to use research analysts to resolve discrepancies in the matching of passenger data to data contained in the database.

However, we have reported that, taken as a whole, the development of Secure Flight has not been effectively managed—has not, in fact, been implemented—and is at risk of failure. We have reported on multiple occasions that the Secure Flight program has not met key milestones, or finalized its goals, objectives, and requirements and have recommended that TSA take numerous steps to help to develop the program. For

---

[30]Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458.

[31]Following the events of September 11, and in accordance with the Aviation and Transportation Security Act's requirement that a computer-assisted passenger prescreening system be used to evaluate all passengers, TSA subsequently began an effort in March 2003 to develop a new computer-assisted passenger prescreening system, known as CAPPS II. Because of a variety of delays and challenges, in August 2004, DHS cancelled the development of CAPPS II. In its place, TSA announced that it would develop a new prescreening program, called Secure Flight.

example, to help manage risk associated with Secure Flight's continued development and implementation, we recommended in March 2005 that TSA finalize the system requirements and develop detailed test plans to help ensure that all Secure Flight system functionality is properly tested and evaluated. We also recommended that TSA develop a plan for establishing connectivity among the air carriers, CBP, and TSA to help ensure the secure, effective, and timely transmission of data for use in Secure Flight operations. In early 2006, TSA suspended development of Secure Flight and initiated a reassessment, or rebaselining, of the program, to be completed before moving forward. Our work reviewing air carriers' current processes has identified two air carriers that are enhancing their identity-matching systems, since it remains unclear when TSA will take over the passenger identity-matching function through Secure Flight. However, any improvements made to the accuracy of an individual air carrier's identity-matching system will not apply system-wide and could further exacerbate differences that currently exist among the various air carriers' systems. These differences may result in varying levels of effectiveness in the matching of passenger names against the terrorist watch list. At Congress's request, we are continuing to monitor TSA's progress to develop Secure Flight. (See app. III for a list of GAO products related to domestic passenger prescreening, including Secure Flight.)

## CBP Faces Challenges Obtaining Data Needed To Prescreen Travelers on International Flights before Takeoff

The ongoing security concerns about prescreening for domestic flights, including disclosure of watch list information outside the government and the quality of information used for the identity-matching process, also pertain to international flights departing from or traveling to the United States. As with domestic passenger prescreening, air carriers conduct an initial match of passenger names against terrorist watch lists—the no-fly and selectee lists—before international flights depart to or from the U.S. using information that passengers supply when they make their reservations. Customs and Border Protection (CBP)—the DHS agency responsible for international passenger prescreening—supplements the identity-matching conducted by air carriers by comparing more reliable passenger information collected from passports against the terrorist watch lists and other government databases for international flights.[32] (This information is considered more reliable because passport data is not self-

---

[32]CBP performs a second name match of passenger names using more reliable data from passenger passports, as well as additional databases to identify other passengers—who may not have been included on the watch lists used by the air carriers—but who nonetheless may be of interest or represent a risk for other reasons, such as past criminal activity, or a prior visa overstay.

reported.) However, the current process does not require the U.S. government's identity-matching procedures be completed prior to the departure of international flights traveling to or from the United States.[33] As a result, passengers thought to be a risk to commercial aviation have successfully boarded flights. For example, in calendar year 2005, a number of passengers previously identified by the U.S. government as direct threats to the security of commercial aviation boarded international flights traveling to or from the United States, according to agency incident reports.[34] In seven cases, the resulting risk was deemed high enough to divert the flight from its intended U.S. destination, resulting in costs to the air carriers, delays for passengers, and government intervention. While none of the flights resulted in an attempted hijacking or other security incidents, these flights nevertheless illustrate a continuing vulnerability that high-risk passengers could potentially board international flights and attempt to blow up these aircraft or take control in order to use them as weapons against U.S. interests at home or abroad.

To address this vulnerability, as part of the Intelligence Reform and Terrorism Prevention Act of 2004, Congress mandated that DHS issue a proposed plan by February 15, 2005, for completing the U.S. government's identity-matching process before the departure of international flights.[35] While CBP did not meet this deadline, the agency issued a proposed rule[36] that would eliminate the preliminary screening conducted by air carriers and replace it instead with a process where air carriers select one of two options for transmitting this information earlier to CBP. One option allows air carriers to transmit passport information as each individual passenger checks in. Under this option, CBP would analyze the information against terrorist watch lists, make an immediate (or "real-time") decision about whether the passenger can board the aircraft, and convey this information electronically to the air carrier. Under this approach air carriers could

---

[33]The government's identity matching process check is often not completed until after a flight departs because air carriers are not required to provide passenger passport data to CBP until 15 minutes before the flight departs for an international flight originating in the United States or 15 minutes after the flight departs for international flights bound for the United States.

[34]The specific number of passengers identified by the U.S. government as direct threats to commercial aviation who boarded international flights is sensitive security information.

[35]Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, §4012, 118 Stat.3638.

[36]CBP published a Notice of Proposed Rulemaking in July 2006.

admit passengers for flights up to 15 minutes before departure. The second option allows air carriers to provide all passengers' passport information (in a bulk data transmission) to CBP for verification at least 60 minutes before a flight's departure. Under either option, the government would retain control of the watch lists, resolving this additional security concern.

Regardless of which proposed option air carriers choose to pursue, many of CBP's efforts to improve the international prescreening process are still largely in development, and the agency faces several challenges in implementing its proposed solutions. One challenge, in particular, concerns stakeholder coordination. CBP must rely on a variety of stakeholders to provide input or to implement aspects of the prescreening process, including air carriers, industry associations, foreign governments, and other agencies within and outside DHS. One coordination challenge involves aligning international aviation passenger prescreening with TSA's development of its Secure Flight program for prescreening passengers on domestic flights. Ensuring that this coordination effort aligns with Secure Flight is important to air carriers, since passengers may have both a domestic and an international part to their itinerary. If these prescreening processes are not coordinated, passengers may be found to be high-risk on one flight and not high-risk on another flight, resulting in air carrier confusion and a potential security hazard. We have recently recommended that DHS take additional steps and make key policy and technical decisions (in order to determine, for example, the data and identity-matching technologies that will be used) that are necessary to more fully coordinate CBP's international prescreening program with TSA's prospective domestic prescreening program, Secure Flight.[37] (See app. III for a list of GAO products related to domestic and international passenger prescreening.)

## GAO Concluding Observations—Passenger Prescreening

While passenger prescreening represents a more secure layer of defense today than it did on 9/11, there is still a need for DHS, TSA, and CBP to follow through on congressional requirements and recommendations we have made to improve the process. Specifically, TSA must still comply with a congressional requirement for transferring responsibility for the passenger identity-matching process from air carriers to TSA for domestic flights. In addition, we made a recommendation in November 2006, which

---

[37]GAO, *Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, But Planning and Implementation Issues Remain*, GAO-07-55SU (Washington, D.C.: November 2006).  We expect to issue a public version of this report in the first quarter of 2007.

DHS has taken under consideration, aimed at helping the agency to enhance coordination between CBP's international prescreening program and TSA's prospective domestic prescreening program, Secure Flight. Such efforts are necessary to help ensure that the prescreening process—as a first layer of aviation defense—is accurate and effective in identifying potential terrorists who should be denied boarding or receive additional screening, and in ensuring that watch list data are not at risk of disclosure to those wishing to do harm to U.S. interests.

## Passenger Checkpoint Screening Threat Detection Capabilities Have Been Strengthened and Efforts to Further Enhance Screener Training, Screening Procedures, and Related Technologies Are Under Way

The layer of aviation security most visible to the general public, as well as to terrorists, is the physical screening of passengers and their carry-on bags at airport checkpoints, known as passenger checkpoint screening. The passenger checkpoint screening process involves the inspection of passengers and their carry-on bags to deter and prevent the carriage of any unauthorized explosive, incendiary, weapon, or other dangerous item on board an aircraft. Checkpoint screening is a critical component of aviation security—and one that has long been subject to security vulnerabilities. Passenger checkpoint screening is comprised of three elements: (1) the people responsible for conducting the screening of airline passengers and their carry-on items; (2) the procedures that must be followed to conduct screening; and (3) the technology used in the screening process. TSA has made progress in implementing security-related measures in all these areas, but there are additional opportunities to further enhance aviation security through the people, processes, and technologies involved in passenger checkpoint screening.

Prior to the passage of ATSA, the screening of passengers had been performed by private screening companies under contract to the air carriers. The FAA was responsible for ensuring compliance with screening regulations. As we reported in 2000, since 1978, the FAA and the airline industry have continued to face challenges in improving the effectiveness of airport checkpoint screeners, and we reported that screeners were not detecting dangerous objects, including loaded firearms and, in tests conducted by FAA, simulated explosive devices. We attributed screening detection problems primarily to high turnover rates among screeners, among other things. By the time the terrorist attacks occurred, the FAA was already 2 years behind in issuing a regulation in response to a congressional mandate requiring the companies that employ checkpoint screeners to improve their testing and training through a certification program.

As the 9/11 Commission report testified, the terrorist hijackers, having escaped watch-list detection during the prescreening process, had to beat

only one layer of security—the security checkpoint process—in order to proceed with their plan. The Commission concluded that at the time of the attacks, while walk-through metal detectors and X-ray machines were in use to stop prohibited items, many potentially deadly and dangerous items—such as the box-cutters carried by the hijackers—did not set off metal detectors or were hard to distinguish in an X-ray machine. Moreover, FAA regulations and guidance did not explicitly prohibit knives with blades under 4 inches long. And the standards for what constituted a deadly or dangerous weapon were "somewhat vague," the commission found, and were left up to the discretion of air carriers and their screening contractors. Moreover, secondary screening—whereby passengers coming through the checkpoint with carry-on bags are selected for additional screening—took place, by and large, only when passengers triggered metal detectors. Even when such trigger events occurred, passengers often were cleared to board. For example, of the 5 hijackers who boarded planes at Washington Dulles International Airport on 9/11, three set off metal detectors; they (and one carry-on bag as well) were hand-wanded, the bag swiped for explosive trace detection, and then they were cleared to board.

**TSA Has Made Progress in Training and Evaluating a Federalized Workforce for Screening Airline Passengers**

After 9/11 and as a result of ATSA, TSA assumed responsibility for screeners and screening operations at more than 400 commercial airports, established a basic screener training program, and has conducted annual proficiency reviews and operational testing of screeners, now known as transportation security officers (TSO). TSA has taken numerous steps to develop and evaluate its screening personnel by, among other things, expanding training beyond the basic training requirement through a self-guided on-line learning center, and by providing additional training on threat information, explosives detection, and new screening approaches. While these efforts and others taken by the agency have helped TSA to develop and evaluate appropriate workforce skills, we have recommended that TSA take additional steps to ensure that this training is delivered. For example, at some airports we have visited, TSOs encountered difficulty accessing and completing recurrent (refresher) training because of technological and staffing constraints. In May 2005, TSA stated that it had a plan for deploying high speed Internet connections at airports. The President's 2007 budget request reported that approximately 220 of the nation's 400 commercial airport and field locations have full information technology infrastructure installation. (See app. III for a list of GAO products related to screener workforce issues.)

**Passenger Checkpoint Screening Procedures Have Been Enhanced to Improve Security and Procedures Are Regularly Modified to Reflect Current Conditions**

In addition to TSA's efforts to train and deploy a federal screener workforce, steps also have been taken to strengthen checkpoint screening polices and procedures to enhance security. One of the most important differences of the current checkpoint screening system compared to the system in place on 9/11 is the additional physical screening that certain passengers selected by the prescreening process, as discussed earlier, must undergo at the checkpoint. In addition, certain screening procedures performed by TSOs, or other authorized TSA personnel, are now mandatory for all passengers. Prior to entering the sterile area of an airport—the area within the terminal where passengers wait to board departing aircraft—all passengers must be screened by a walk-through metal detector and their carry-on items must be X-rayed. Passengers whose carry-on baggage alarms the x-ray machine, passengers who alarm the walk-through metal detectors, or passengers who are selected by the air carriers' passenger prescreening system,[38] all receive additional screening. These passengers may be screened by hand-wand or pat-down or have their carry-on items screened for explosive traces or physically searched. Figure 2 shows the functions performed as part of passenger checkpoint screening.

---

[38]Passengers also may be selected for additional scrutiny randomly or by other TSA-approved processes.

**Figure 2: Passenger Checkpoint Screening Functions**
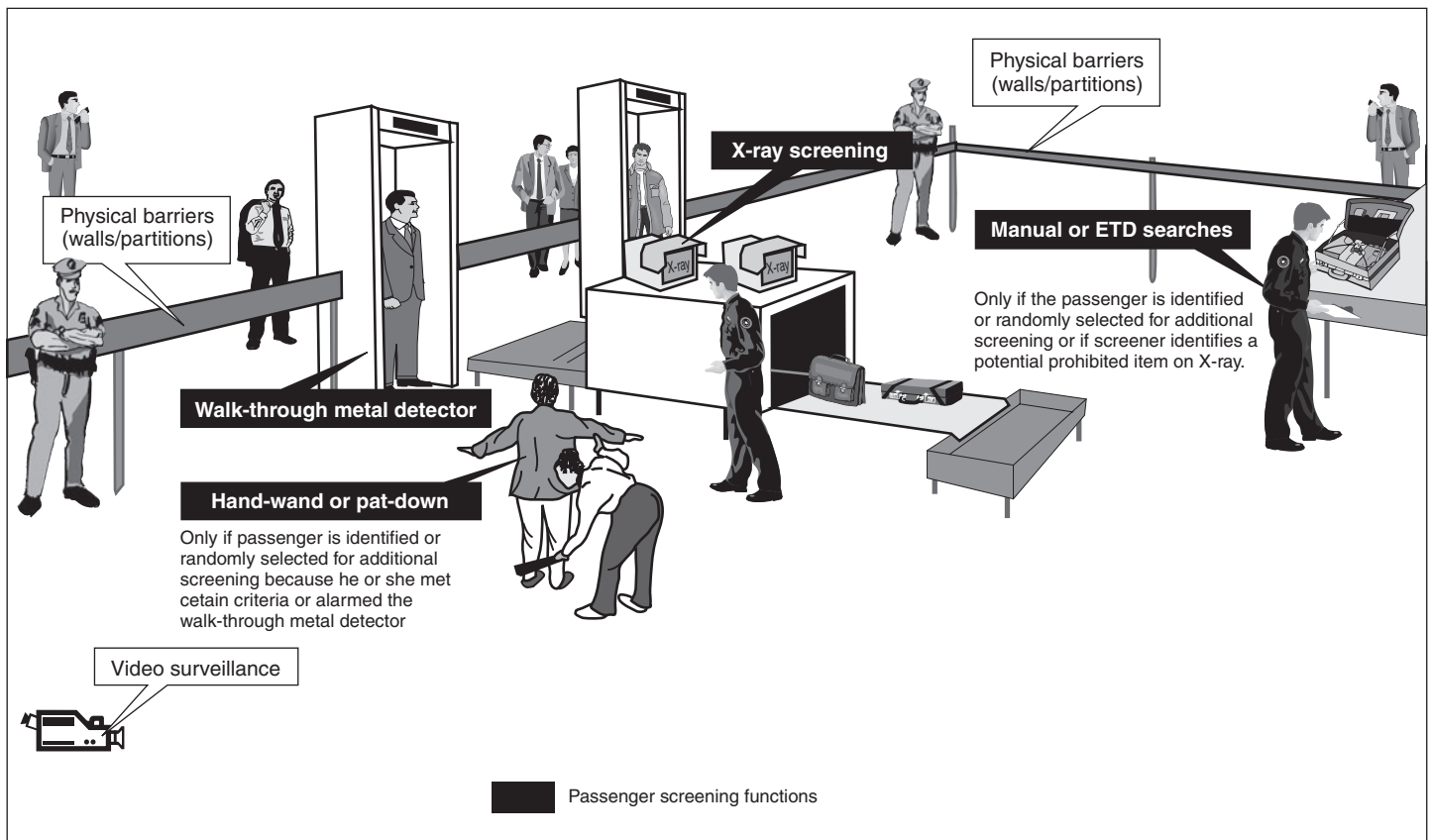


Source: GAO and Nova Development Corporation.

Note: ETD refers to explosive trace detection equipment in which bags are swabbed to test for chemical traces of explosives.

Because history has shown that terrorists will adapt their tactics and techniques in an attempt to bypass increased security procedures, and are capable of developing increasingly sophisticated measures in an attempt to avoid detection, TSA leadership has emphasized the need to continually test or implement new screening procedures to further enhance security in response to changing conditions. We have ongoing work on how TSA modifies and implements passenger checkpoint screening procedures and plan to issue a report in February 2007. Last year, we testified that TSA security-related proposed changes to checkpoint screening procedures are based on risk-based factors, including previous terrorist incidents, threat information, vulnerabilities of the screening system, as well as operational experience and stakeholder concerns.

Recommended modifications to passenger checkpoint screening procedures are also generated based on covert testing conducted by TSA officials and the DHS Office of Inspector General (OIG). Covert tests are designed to assess vulnerabilities in the checkpoint screening system to specific threats, such as vulnerability to the various methods by which terrorists may try to conceal handguns, knives, and improvised explosive devices (IED). We have ongoing work evaluating TSA's covert testing efforts and expect to report our results later this year.

**TSA Is Exploring New Technologies to Enhance Detection of Explosives and Other Threats**

The ever changing terrorist threat also necessitates continued research and development of new technologies and the fielding of these technologies to strengthen aviation security. The President's fiscal year 2007 budget request notes that emerging checkpoint technology may enhance the detection of prohibited items, especially firearms and explosives, on passengers. Furthermore, the DHS OIG has reported that significant improvements in screener performance may not be possible without greater use of new technology, and has encouraged TSA to expedite its technology testing programs and give priority to technologies that will enable screeners to better detect both weapons and explosives.[39] TSA has recently put increased focus on the threats posed by IEDs and is investing in technology for this purpose. For example, since the September 11 attacks, 94 explosive-detection-trace portal machines have been installed at 37 airports. (These machines detect vapors and residues of explosives, including IEDs.) In addition, as of May 2006, TSA had conducted, or planned to conduct, evaluations of nine new types of passenger screening technology, including, for example, technology that would screen bottles for liquid explosives. It is important that TSA continue to invest in and develop technologies for detecting explosives This is especially important in light of the alleged August 2006 plot to detonate liquid explosives on board multiple commercial aircraft bound for the United States from the United Kingdom. We are currently evaluating DHS's and TSA's progress in planning for, managing, and deploying research and development programs in support of airport checkpoint screening operations. We expect to report our results later this

---

[39]Follow-Up Audit of Passenger and Baggage Screening Procedures at Domestic Airports (Unclassified Summary). Department of Homeland Security Office of Inspector General, OIG-05-16. Washington, D.C.: March 2005.

year. (See app. III for a list of GAO products related to passenger checkpoint screening.)

GAO Concluding
Observations—Passenger
Checkpoint Screening

As with passenger prescreening, the checkpoint screening system in place today is far more robust, reflects more rigorous screening requirements, and deploys better trained staff, than in the years leading up to the terrorist attacks. In its list of recommended actions that the government should take to protect against and prepare for future terrorist attacks, the 9/11 Commission suggested that improving checkpoint screening should be a priority. TSA has largely accomplished this goal, though as with all aspects of aviation security, efforts to further enhance and strengthen procedures are ongoing. For example, new and emerging technologies for detecting threat objects are likely to help enhance the checkpoint screening process.

In-flight Security Measures in
Preparing For or Responding
To On-board Threats, and
Coordinating Responses from
the Ground, Have Been
Strengthened

Security protocols and policies for preparing for or responding to threats that occur on board flights already in progress, and coordinating responses to such security events from the ground, have changed significantly since 9/11. With respect to on-board security measures, the airline cabin and flight crews on duty on 9/11 were neither trained for nor prepared to deal with the events that unfolded once the hijackers were on board. Though in-flight security was regarded as a layer of defense in the commercial aviation system, FAA's security training guidelines at the time did not contemplate suicide hijackers, with aircraft used as guided missiles, as a likely scenario. Flight crews had been taught to cooperate, rather than resist, during an emergency. As with the prescreening and checkpoint screening processes, the ability of the hijackers to manipulate flight crews and penetrate the captain's cockpit revealed serious weaknesses of in-flight security.

In-flight security has since been strengthened in several ways to help mitigate the likelihood of terrorists being able take over an aircraft. For example, TSA established the Federal Flight Deck Officer program in 2002. The program trains eligible flight crew members in the use of force to defend against an act of criminal violence or air piracy. These flight deck officers are deputized as federal law enforcement officers, and may transport and carry a TSA-issued firearm, in a manner approved by TSA. In

addition, FAA directed air carriers to harden their cockpit doors[40] and Congress expanded the decades-old Federal Air Marshal Service by mandating in ATSA the deployment of air marshals, on board all high-security risk flights. Before 9/11, there were 33 air marshals altogether; now there are thousands.[41] A key aspect of air marshals' operating procedures is the discreet (semicovert) movement through airports as they check in for their flight, transit screening checkpoints, and board the aircraft.

TSA has also taken steps to ensure that flight and cabin crew members—among the last lines of defense—are prepared to handle potential threat conditions on board commercial aircraft. The revised guidance and standards TSA developed for air carriers to follow in developing and delivering their flight and cabin crew member security training is a positive step forward in strengthening the security on board commercial aircraft. This training includes, among other things, teaching crew members how to search a cabin for explosive devices. Congress also mandated TSA to implement an advanced voluntary crew member self-defense training program for flight and cabin crew members; this training is ongoing.

With respect to coordinating responses to on-board threats from the ground, the events of 9/11 revealed the importance of prompt interagency communication to allow for a unified, coordinated response to airborne threats. Once an in-flight security threat is identified, rapid and effective information sharing among agencies on the ground is critical to ensure that each agency can respond according to its mission and that the security threat is handled in the safe manner. The 9/11 Commission Report stated that a weakness in aviation security exploited by the terrorists included a lack of protocols and capabilities in executing a coordinated FAA and military response to multiple hijackings and suicidal hijackers.

---

[40]The Intelligence Reform and Terrorism Prevention Act of 2004 included a provision to study the use of secondary flight deck barriers as a means of protecting the airline cockpit when the door is opened during in-flight meal service, or when a pilot needs to leave the cockpit. No airline has yet implemented such barriers but United Airlines is considering such a measure.

[41]The U. S. Federal Air Marshal Service has undergone a number of organizational changes since its creation, including moving from FAA to TSA in November 2001 and from DOT to DHS in March 2003. Several months later, the air marshals were transferred from TSA to U.S. Immigration and Customs Enforcement and in 2005 were transferred back to TSA. The exact number of air marshals is considered classified information.

According to the commission, the response on 9/11 of the Department of Defense's North American Aerospace Defense Command (NORAD), which is responsible for securing U.S. airspace, was hindered in part by lack of real-time communications with FAA and defense and intelligence agencies. For instance, a shootdown authorization was not communicated to the NORAD air defense sector until 28 minutes after United 93 had crashed in Pennsylvania.[42] Moreover, the commission noted, planes did not know where to go or what targets they were to intercept. And once the shootdown order was given, it was not communicated to the pilots.

To address the communications and coordination problems that were highlighted by 9/11, many federal agencies, including the FAA, DOD, and TSA, have taken action. For example, the FAA—which is responsible for managing aircraft traffic entering into or operating in U.S. airspace—established an unclassified teleconference system, called the Domestic Events Network, designed to gather and disseminate information for all types of security threats. The network is monitored by approximately 60 users from a variety of federal agencies as well as state and local entities. This network was originally established as a conference call on the morning of 9/11 to coordinate the federal response to the hijacked aircraft and it has remained in existence since then, serving as a basis for interagency cooperation. Any Domestic Events Network user can broadcast information, allowing other agencies on the Network to communicate and monitor a situation in real-time.[43] According to FAA officials, domestic air carriers have recently been given the capability to link into the Domestic Events Network, allowing for the air carrier to provide real-time situational updates as they are received from the flight crew onboard the aircraft in question without relying on an intermediary party. Another important interagency communications tool is the Defense Red Switch Network which is a secure, classified network administered by the DOD that allows multiple agencies to discuss intelligence information over a secure line.[44]

---

[42]NORAD has since increased its level of air patrols and use of early warning aircraft.

[43]Events broadcast over the Domestic Events Network may include incidents that occur in an airport terminal as well as situations that arise onboard an airplane.

[44]Noble Eagle is one example of a classified teleconference that occurs on the Defense Red Switch Network. Noble Eagle conferences are initiated by DOD, though other agencies can request that a Noble Eagle conference be convened.

In addition, TSA has established the Transportation Security Operations Center (TSOC), a national center that operates around the clock and coordinates the multi-agency response to in-flight security threats. Air carriers are required to report to TSOC all incidents and suspicious activity that could affect the security of U.S. civil aviation, including any incidents of interference with a flight crew, specific or non-specific bomb threats, and any correspondence received by an aircraft operator that could indicate a potential threat to civil aviation. We have ongoing work analyzing the processes that federal agencies follow to identify, assess, and respond to in-flight security threats and the extent to which interagency coordination problems occurred, if at all, and the steps agencies took to address identified problems. The results of this work, which will be issued in early 2007, will be classified. (See app. III for a list of GAO products related to in-flight security.)

## GAO Concluding Observations—In-flight Security and Ground-Based Response Efforts

Several actions taken in the months after 9/11—notably, hardened cockpit doors, better emergency response training for airborne flight crews, and the presence of federal air marshals on certain flights—have helped to ensure that aircraft are both physically safer and better protected from the actions of on-board hijackers or terrorists. Federal actions also have been taken in response to the communications and coordination failures that occurred on 9/11 in order to enhance coordinated responses to onboard security threats from the ground. Our ongoing work will discuss, among other things, the process federal agencies follow to identify, assess, and respond to security threats, and the challenges, if any, that have arisen in agencies' coordination efforts and steps taken to deal with them.

## Areas of Aviation System Not Exploited by 9/11 Terrorists Also Have Been Strengthened, though Implementation and Resource Challenges Remain

Two aspects of commercial aviation that were not directly implicated in the 9/11 scenario—checked baggage screening and air cargo screening—are nonetheless recognized as important components of a layered system of aviation defense. Congress and TSA have taken steps to enhance the security of both in the years since 9/11, though resource and technology challenges remain. The infrastructure of commercial airport properties, which can pose risks to security by enabling criminals or terrorists to penetrate sensitive areas (such as boarding areas or baggage facilities), also has received congressional and federal attention. In addition, Congress and federal agencies have taken actions to enhance security in the noncommercial aviation sector, specifically, at the nation's general aviation airports—small airports that are home to flight training schools as well as privately owned aircraft.

**TSA Has Installed Baggage Screening Explosive Detection Equipment at Most Airports and Has Begun to Identify Costs, Benefits, and Technologies for Further Optimizing Baggage Screening**

With respect to checked baggage screening, at the time of the attacks, there was no federal requirement to screen all checked baggage on domestic flights. In some cases, air carriers screened checked baggage on commercial flights for bulk quantities of explosives using X-ray screening equipment similar to that used for medical CAT scans. As the Congressional Research Service reported a month after the attacks, the availability and cost of baggage screening X-ray equipment, along with the time it took to screen a bag, did not permit its use in all airports, on all flights at airports where it was used, or even on all bags on any given flight. In addition, passengers selected by the passenger prescreening process for additional pre-flight scrutiny were either to have their checked bags scanned for explosives or held until they boarded the aircraft. As noted earlier, 5 of the 8 hijackers selected by the passenger prescreening system in place on 9/11 had their checked bags held prior to boarding and three had their bags scanned for explosives.

After the attacks, Congress, through ATSA, mandated that all checked baggage at commercial airports be screened using explosive detection systems.[45] TSA has worked to overcome equipment challenges, and other challenges, in order to fulfill this mandate, and now reports having the capability to screen 100 percent of checked baggage using two types of screening equipment—explosive detection systems (EDS), which use X-rays to scan bags for explosives, and explosive trace detection systems (ETD), in which bags are swabbed to test for chemical traces of explosives. TSA considers screening with EDS to be superior to screening with ETD because EDS machines process more bags per hour and automatically detect explosives without direct human involvement.[46] As of June 2006, in order to screen all checked baggage for explosives at over 400 airports, TSA had procured and installed about 1,600 EDS and 7,200 ETD machines.

TSA has begun shifting its focus away from placing these systems primarily in airport lobbies, as had been done initially, because of problems that arose from this configuration. For instance, TSA's

---

[45]Checked baggage screening primarily involves the inspection of checked baggage to deter, detect, and prevent the carriage of any unauthorized explosive, incendiary, or weapon on board an aircraft.

[46]TSA also uses alternative screening procedures to screen checked baggage for explosives for certain short-term circumstances that involve some form of explosives detection as well as other methods that do not use either EDS or ETD, such as canine screening.

placement of stand-alone EDS and ETD machines in airport lobbies resulted in passenger crowding, which presented unsafe conditions and may have added security risks for passengers and airport workers. TSA has begun to focus instead on systematically deploying the configuration of baggage screening equipment that is considered by TSA to be the most efficient, least labor-intensive, and most cost-effective at many airports—in-line EDS. These systems are integrated with airports' baggage conveyor and sorting systems (see fig. 3 for an illustration of the checked-baggage screening system using an in-line EDS machine). TSA has also developed smaller and less expensive stand-alone EDS equipment that may be effective at smaller airports or closer to airline check-in counters.

**Figure 3: In-line Checked Baggage Screening System**
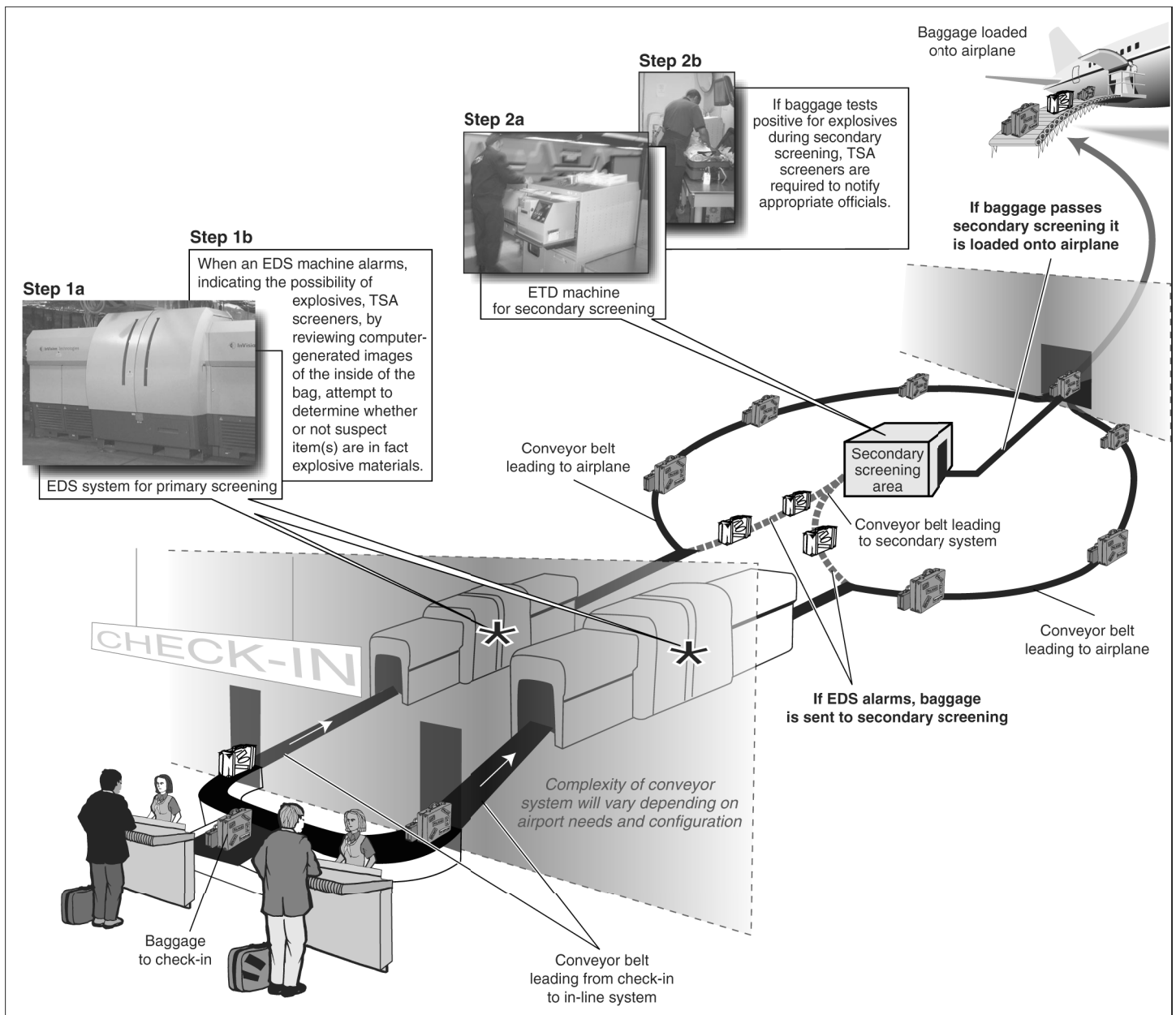


Source: GAO and Nova Development Corporation.

A TSA cost-benefit analysis of in-line EDS machines being installed at nine airports conducted in May 2004 showed that they could yield significant savings for the federal government and achieve other benefits—including

reduced screener staffing requirements and increased baggage throughput (the rate at which bags are processed). Specifically, TSA estimated that in-line baggage screening systems at these nine airports could save the federal government about $1 billion over 7 years.

The Intelligence Reform and Terrorism Prevention Act of 2004 mandated and the conference report accompanying the fiscal year 2005 DHS Appropriations Act directed TSA to, among other things, develop a comprehensive plan for expediting the installation of in-line explosive detection systems. To assist TSA in planning for the optimal deployment of checked baggage screening systems, we recommended in March 2005 that TSA systematically evaluate baggage screening needs at airports, including the costs and benefits of installing in-line EDS systems at airports that did not yet have such systems installed. We suggested that such planning should include analyzing which airports should receive federal support for in-line EDS systems based on cost savings that could be achieved from more effective and efficient baggage screening operations and on other factors, including enhanced security. And we recommended that TSA identify and prioritize the airports where the benefits of replacing stand-alone baggage screening systems with in-line systems are likely to exceed the costs of the systems, or where the systems are needed to address security risks or related factors.

In February 2006, in response to our recommendation and a legislative requirement to submit a schedule for expediting the installation and use of in-line systems and replacement of ETD equipment with EDS machines,[47] TSA provided to Congress its strategic planning framework for its checked baggage screening program. This framework introduced a strategy intended to increase efficiency through deploying EDS to as many airports as practicable, lowering lifecycle costs for the program, minimizing impacts to TSA and airport/airline operations, and providing a flexible security infrastructure for accommodating growing airline traffic and potential new threats. The framework is an initial step toward: (1) finding the ideal mix of higher-performance and lower-cost alternative screening solutions for the 250 airports with the highest checked baggage volumes, and (2) funding prioritization schedules by airport, by identifying the top 25 airports that should first receive federal funding for projects related to

---

[47]Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 4019, 118 Stat/ 3638, 3721-22.

the installation of EDS based on quantitative modeling of security and economic factors, and other factors.[48]

In addition, partly in response to other recommendations we made, TSA is collaborating with airport operators, air carriers, and other key stakeholders to identify funding and cost sharing strategies (in order to determine how to allocate investments in baggage equipment between the federal government and air carriers) and is focusing its research and development efforts on the next generation of EDS technology. For airports where in-line systems may not be economically justified because of high investment costs, we suggested that a cost-effectiveness analysis be used to determine the benefits of additional stand-alone EDS machines to screen checked baggage in place of the more labor-intensive ETD machines. According to TSA, the agency is conducting an analysis of the airports that rely heavily on ETD machines and determined if they would benefit from also having stand-alone EDS equipment. (See app. III for a list of GAO products related to checked baggage screening.)

## TSA Has Strengthened Oversight and Inspection of Air Cargo but We Have Reported That More Work Is Needed to Ensure Shippers Comply with Security Requirements and Address Potential Resource Challenges

In the aftermath of the 9/11 terrorist attacks, the security of cargo carried on both passenger and all-cargo aircraft became a growing concern both to the public and to members of Congress. Since the attacks, several instances of human stowaways in the cargo holds of all-cargo aircraft have further heightened the concern over air cargo security by revealing vulnerabilities that could potentially threaten the entire air transportation system.

TSA has the responsibility for ensuring the security of air cargo, including, among other things, establishing security rules and regulations covering domestic and foreign passenger carriers that transport cargo, domestic and foreign all-cargo carriers, and domestic indirect air carriers (companies that consolidate air cargo from multiple shippers and deliver it to air carriers to be transported); and has responsibility for overseeing implementation of air cargo security requirements by air carriers and indirect air carriers through compliance inspections. In general, TSA inspections are designed to ensure that air carriers comply with air cargo

---

[48]A congressionally established Aviation Security Capital Fund for baggage screening investments has a mandatory funding level of $250 million annually and there is an additional authorization for up to $400 million per year, through fiscal year 2007. Congress also gives TSA the authority to issue letters of intent to airports, committing future funding toward in-line EDS integration projects.

security requirements, while air carrier inspections focus on ensuring that cargo does not contain weapons, explosives, or stowaways (see fig. 4).

**Figure 4: Air Cargo Being Loaded and Inspected Using an Explosive Detection System**



Source: GAO.



Source: TSA.

Because safeguarding the nation's air cargo transportation system is a shared public and private sector responsibility, air carriers are generally responsible for meeting TSA's air cargo security requirements, including how employees are to handle and physically inspect cargo.

As we reported in October 2005, TSA has implemented a variety of actions intended to strengthen oversight for domestic air cargo security operations conducted by air carriers.[49] For air cargo, TSA has increased the number of dedicated air cargo inspectors used to assess air carrier and indirect air carrier compliance with security requirements, issued a regulation in May 2006 to enhance and improve the security of air cargo transportation, and has taken other actions. However, our work identified factors that may limit the effectiveness of these measures. For example:

---

[49]GAO, *Aviation Security: Federal Action Needed to Strengthen Domestic Air Cargo Security*, GAO-06-76 (Washington, D.C.: October 2005).

- TSA has primarily relied on its Known Shipper program[50] (allowing individuals or businesses with established histories to ship cargo on passenger carriers) to ensure that cargo transported on passenger air carriers is screened in accordance with ATSA, and that unknown shipments are not placed on passenger aircraft. However, at the time of our review, we reported that the Known Shipper program had weaknesses and may not provide adequate assurance that shippers are trustworthy and that air cargo transported on passenger air carriers was secure. For example, the information in TSA's database on known shippers was incomplete because participation was voluntary, and the information in the database may not have been reliable. TSA has addressed this issue through its May 2006 regulation on air cargo security requirements, making it mandatory for air carriers and indirect air carriers to provide information to this database by requiring them to submit data on their known shippers.

- TSA established a requirement for random inspection of air cargo reflecting the agency's position that inspecting 100 percent of air cargo was not technologically feasible and would be potentially disruptive to the flow of air commerce. However, this requirement contained exemptions based on the nature and size of cargo that may leave the air cargo system vulnerable to terrorist attack. We recommended in 2005 that TSA reexamine the rationale for existing air cargo inspection exemptions, determine whether such exemptions leave the air cargo system unacceptably vulnerable to terrorist attack, and make any needed adjustments to the exemptions. In September 2006, TSA revised the criteria for exemptions for cargo transported within or from the United States on passenger aircraft. TSA is reviewing the remaining inspection exemptions to determine whether or not they pose an unacceptable vulnerability to the air cargo transportation system.

- TSA conducts audits of air carriers and indirect air carriers to ensure that they are complying with existing air cargo security requirements. But TSA has not developed performance measures to determine to what extent air carriers and others are complying with air cargo security requirements. Without performance measures to gauge air carrier and indirect air carrier compliance with air cargo security requirements, TSA cannot effectively focus its inspection resources on those entities posing the greatest risk. In addition, without measures to

---

[50]The Known Shipper program was created prior to the events of September 11 to establish procedures for differentiating between shippers that are known and unknown to an indirect air carrier or air carrier.

determine an acceptable level of compliance with air cargo security requirements, TSA cannot assess the performance of individual air carriers or indirect air carriers against national performance averages or goals that would allow TSA to target inspections and other actions on those that fall below acceptable levels of compliance. We recommended that TSA assess the effectiveness of enforcement actions, including the use of civil penalties, in ensuring air carrier and indirect air carrier compliance with air cargo security requirements. We also recommended that TSA develop measures to gauge air carrier and indirect air carrier compliance with air cargo security requirements to assess and address potential security weaknesses and vulnerabilities.

- TSA had not analyzed the results of air cargo security inspections to systematically target future inspections on those entities that pose a higher security risk to the domestic air cargo system, or assessed the effectiveness of its enforcement actions in ensuring air carrier compliance with air cargo security requirements. Such targeting is important because TSA may not have adequate resources to inspect all air carriers and indirect air carriers on a regular basis. We recommended that TSA develop a plan for systematically analyzing the results of air cargo compliance inspections and use the results to target future inspections and identify systemwide corrective actions. According to TSA officials, the agency has been working on developing short-term and long-term outcome measures for air cargo security and has begun to analyze inspection results to target future inspections.

Finally, with respect to TSA's regulation on air cargo security requirements, in May 2006, TSA estimated that implementing all the provisions in the regulation (including actions already ongoing, such as requiring air carriers to randomly inspect a percentage of air cargo) will cost approximately $2 billion over a 10-year period (2005-2014). Before the regulation was finalized, industry stakeholders representing air carriers and airport authorities had stated that several of the provisions, such as securing air cargo facilities, screening all individual persons boarding all-cargo aircraft, and conducting security checks on air cargo workers, would be costly to implement.

We have not assessed how this regulation, or its costs, may affect TSA or stakeholders. Nor have we undertaken additional work to determine the extent to which TSA's subsequent actions have addressed the weaknesses identified above and our related recommendations. In our work, we concluded that while the cost of enhancing air cargo security can be significant, the potential costs of a terrorist attack, in terms of both the loss of life and property and long-term economic impacts, would also be

significant although difficult to predict and quantify. TSA's regulation also covers inbound air cargo security requirements (for cargo originating outside the United States). We currently have an ongoing review assessing the security of inbound air cargo, including the regulation's relevant requirements, and expect to issue this work early this year.

## Security of Commercial Airport Perimeters and Other Secure Areas Are Being Addressed

Like most other aspects of the aviation system, the security of commercial airport facilities also came under heightened scrutiny after 9/11. Congress included provisions in ATSA to address this aspect of airport security. In particular, ATSA granted TSA the authority to oversee U.S. airport operators' efforts to maintain and improve the security of airport perimeters (such as airfield fencing and access gates), the adequacy of controls restricting unauthorized access to secured areas (such as building entry ways leading to aircraft), and security measures pertaining to individuals who work at airports. Apart from ongoing concerns about the potential for terrorists to gain access to these areas, in 2004, concerns also were raised about security breaches and other illegal activities, such as drug smuggling, taking place at some airports. These events highlighted the importance of strengthening security in these areas. Taken as a whole, airport perimeter security and related areas, along with passenger and baggage screening, comprise key elements of the aviation security environment at commercial airports.

We reported in 2004 that TSA had begun evaluating commercial airport security by conducting compliance inspections, among other things, but needed a better approach for assessing how the results of these efforts would be used to make improvements to the entire commercial airport system.[51] We also reported that TSA had helped some airport operators to enhance perimeter and access control security by providing funds for security equipment, such as electronic surveillance systems. However, TSA had not, at the time of our review, set priorities for these and other efforts or determined how they were to be funded. We also found that while TSA had taken some steps to reduce the potential security risks posed by airport workers, the agency did not require fingerprint-based criminal history checks for all workers, as ATSA required. To help ensure that TSA is able to articulate and justify future decisions on how best to proceed with security evaluations, fund and implement security

---

[51]GAO, *Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls*, GAO-04-728 (Washington, D.C.: June 2004).

improvements (including new security technologies), and implement additional measures to reduce the potential security risks posed by airport workers, we recommended that TSA develop a plan for Congress describing how it would meet the applicable requirements of ATSA.

Since our report was issued, TSA made several improvements in these areas, through the issuance of a series of security directives that required enhanced background checks and improved access controls for airport employees who work in restricted airport areas. We have new work planned in this area that will, among other things, examine TSA's further progress in meeting ATSA requirements for reducing the potential security risks posed by airport workers, such as requiring fingerprint-based criminal history checks and security awareness training for all airport workers. We have also recently issued work examining progress toward establishing the Transportation Workers Identification Credential (TWIC) Program.[52] TWIC is intended to establish a uniform identification credential for 6 million workers who require unescorted physical or cyber access to secured areas of transportation facilities, including airports. While TWIC was initially intended to meet an ATSA recommendation that TSA consider using biometric access control systems to verify the identity of individuals who seek to enter a secure airport, as of September 2006, TSA had determined that TWIC would be implemented first for workers requiring unescorted access to secure areas at commercial seaports[53] and that there were no immediate plans to implement the program in the airport environment.

## Federal Regulations Issued After 9/11 Requiring Background Checks for Airline Pilots, and Other Measures, Have Enhanced Security at General Aviation Airports

General aviation, as distinguished from commercial aviation, encompasses a wide variety of activities, aircraft types, and airports.[54] Federal intelligence agencies have reported in the past that terrorists have considered using general aviation aircraft for terrorist acts—and that the 9/11 terrorists learned to fly at flight schools based at general aviation airports in Florida, Arizona, and Minnesota. We have noted in our work

---

[52]GAO, *Transportation Security: DHS Should Address Key Challenges Before Implementing the Transportation Worker Identification Program*, GAO-06-982 (Washington, D.C.: September 2006).

[53]The Maritime Transportation Security Act of 2002 required the Secretary of DHS to issue a maritime worker identification card that uses biometrics, such as fingerprints, to control access to secure areas of seaports and vessels.

[54]There are approximately 14,000 private-use and 4,800 public-use general aviation airports in the United States, and about 550,000 active general aviation pilots and instructors.

that the extent of general aviation's vulnerability to terrorist attack is difficult to determine. Nevertheless, as we reported in November 2004, TSA and the FAA have taken steps to address security risks to general aviation through regulation and guidance.[55] For example, TSA has promulgated regulations requiring background checks of foreign candidates for U.S. flight training schools and has issued security guidelines for general aviation airports. Prior to the September 11 attacks, FAA did not require background checks of anyone seeking a pilot's license. Other measures taken to enhance general aviation security since then include actions by nonfederal general aviation stakeholders who have partnered with the federal government and have individually taken steps to enhance general aviation security. For example, industry associations developed best practices and recommendations for securing general aviation, and have worked with TSA to develop other security initiatives.

While these actions represent progress toward enhancing general aviation security, at the time we reported on these efforts, TSA continued to face challenges. Although TSA has issued a limited assessment of threats associated with general aviation, a systematic assessment of threats to, or vulnerabilities of general aviation to determine how to better prepare against terrorist threats, had not been conducted at the time of our November 2004 review because the assessments were considered costly and impractical to conduct at the nearly 19,000 general aviation airports. We recommended that TSA develop and implement a plan to identify threats and vulnerabilities and include, among other things, estimates of funding requirements. Should TSA establish new security requirements for general aviation airports, competing funding needs could challenge the ability of general aviation airport operators to meet these requirements. General aviation airports have received some federal funding for implementing security upgrades since September 11, but have funded most security enhancements on their own. General aviation stakeholders we contacted expressed concern that they may not be able to pay for any future security requirements that TSA may establish. In addition, TSA and FAA are unlikely to be able to allocate significant levels of funding for general aviation security enhancements, given competing priorities of commercial aviation and other modes of transportation. (We made no recommendations related to funding challenges.) We have not undertaken

---

[55]*General Aviation Security: Increased Federal Oversight Is Needed, but Continued Partnership with the Private Sector Is Critical to Long-Term Success,* GAO-05-144 (Washington, D.C.: November 2004).

additional work to determine the extent to which subsequent actions taken by DHS or TSA have enhanced general aviation security or have addressed our recommendations.

## GAO Concluding Observations—Enhancing Security of Layers of Aviation Defense Not Implicated on 9/11

TSA's efforts to address aspects of aviation security other than those directly implicated in the 9/11 attacks have been mixed. On the one hand, TSA has made significant progress in an area where it has direct operational authority—enhancing detection of threat objects in passengers' checked baggage. Thanks to the increased use of technology (explosive detection systems), today's checked baggage undergoes far more scrutiny than before the terrorist attacks. In other areas of aviation, however, where TSA has regulatory and oversight responsibility, but does not take the operational lead, our past work indicates that TSA faced challenges. With respect to air cargo, for example, TSA has implemented a variety of actions intended to strengthen oversight for domestic air cargo security operations conducted by air carriers, including increasing the number of inspectors used to assess air carriers' compliance with air cargo security requirements, but opportunities exist to better ensure that this compliance process is working. Because we do not have recent work on progress made to enhance the security at general aviation airports, we cannot comment further on the extent of progress made in this area. Our ongoing work on airport perimeter security and access controls will allow us to provide an updated assessment of progress later in 2007.

## Congress and Federal Agencies Are Addressing Security Needs of Transportation Modes in the Post-9/11 Era through Legislation, Risk Management, and Enhanced Cooperation with Domestic and International Partners

In the aftermath of the attacks on 9/11, Congress and the administration focused their energies first on shoring up our national layers of defense—particularly in the aviation sector, which had proven to be vulnerable to terrorist attacks. As of November 2006, TSA had substantially implemented the major aviation security mandates issued by Congress following the 9/11 attacks, particularly those ATSA mandates designed to address specific vulnerabilities exploited by the terrorists, such as the requirement to deploy federal personnel to screen passengers and baggage at airports. Congress, the 9/11 Commission, federal agencies, and we have recognized the need to develop strategies and take actions to protect against and prepare for terrorist attacks on critical parts of our transportation system other than aviation, which also are considered vulnerable to attack. These areas include passenger rail and the maritime industry—both considered vital components of the U.S. economy.[56] In

---

[56]We have work under way on another nonaviation transportation mode—surface transportation—focusing on the security of the motor carrier industry.

GAO-07-375 Progress to Address Security After 9/11

addition, other modes of transportation also remain vulnerable to attack, such as the nation's highway infrastructure and commercial vehicles.

## Multiple Federal Agencies Have Taken Actions to Enhance Passenger Rail Security

The passenger rail sector is one critical area of transportation where a number of federal departments and their component agencies have begun taking actions to enhance security. The U.S. passenger rail sector is a vital component of the nation's transportation infrastructure, with subway and commuter rail systems, among others, carrying more than 11 million passengers each week day.[57] Characteristics of some passenger rail systems—high ridership, expensive infrastructure, economic importance, and location (e.g., large metropolitan areas or tourist destinations)—make them attractive targets for terrorists because of the potential for mass casualties and economic damage and disruption. Indeed, public transportation in general, and passenger rail in particular have continued to be attractive targets for terrorist attack as evidenced by the March 2004 terrorist bomb attacks on commuter trains in Madrid, Spain in which 191 people were killed and 600 injured, and the July 2005 bomb attacks on the London's subway system, which resulted in over 50 fatalities and more than 700 injuries.

Prior to the creation of TSA in 2002, the Federal Transit Administration (FTA) and Federal Railroad Administration (FRA) were the primary federal agencies involved in passenger rail security matters, and both undertook numerous initiatives both before and after 9/11 to enhance security. For example, FTA conducted security readiness assessments of rail transit systems, sponsored security training, and developed security guidance for transit agencies. FRA has assisted commuter railroads and Amtrak in developing security plans, conducted security inspections of commuter railroads, and researched various security technologies, among other things. Since taking over as the lead federal agency responsible for transportation security, TSA has also taken a number of actions intended to enhance passenger rail security. For example, in response to the commuter rail attacks in Madrid, and federal intelligence on potential threats against U.S. passenger rail systems, TSA issued security directives for rail operators in May 2004. The directives required rail operators to implement a number of general security measures, such as conducting frequent inspections of stations, terminals, and other assets, or utilizing canine explosive detection teams, if available. The issuance of these

---

[57]The U.S. passenger rail system consists of heavy rail (such as subways), commuter rail (such as regional commuter lines), light rail, and intercity rail (Amtrak).

GAO-07-375  Progress to Address Security After 9/11

directives was an effort to take swift action in response to a current threat. However, as we reported in September 2005, because these directives were issued with limited input and review by rail industry and federal stakeholders, they may not provide the industry with baseline security standards based on industry best practices.[58] Furthermore, no permanent rail security standards had been promulgated and clear guidance for rail operators was lacking. To ensure that future rail security directives are enforceable, transparent, and feasible, we recommended that TSA collaborate with the Department of Transportation and the passenger rail industry to develop rail security standards that reflect industry best practices and that can be measured, monitored, and enforced. Among other actions taken, TSA has also tested emergency rail security technologies for screening passenger baggage and has enlarged its national explosives detection canine program to train and place canine teams in the nation's mass transit and commuter rail systems. (See app. III for information on GAO products related to passenger rail security.)

## TSA Has Identified the Nation's Highway Infrastructure and Commercial Vehicles as Vulnerable to Terrorist Attack

In addition to the U.S. passenger rail system, concerns have been raised about the nation's highway infrastructure, which facilitates transportation for a vast network of interstate and intrastate trucking companies and others. Vehicles and highway infrastructure play an essential role in the movement of goods, services, and people, yet more work needs to be done to assess or address vulnerabilities to acts of terrorism that may exist in these systems. Surface transportation provides terrorists with thousands of points from which to attack and easy escape routes, potentially causing significant loss of life and economic harm. Indeed, threat information and TSA assessments have identified that specific components of the commercial vehicle sector are potential targets—and are vulnerable—to terrorist attacks. Among other targets, attackers can target bridges, tunnels, and trucks, including using hazardous material trucks as weapons. Further, the diversity of the trucking industry poses additional challenges in effectively integrating security in both large, complex trucking operations and smaller owner/operator businesses. We have work under way to analyze federal efforts to strengthen the security of commercial vehicles, including vehicles carrying hazardous materials, and how federal agencies coordinate their efforts to secure the commercial vehicle sector. We expect to report on this work later this year.

---

[58]*Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO-05-851 (Washington, D.C.: September 2005).

## Federal Agencies and Stakeholders Have Taken Steps to Identify and Reduce Vulnerabilities and Enhance Security at Seaports

The maritime sector is another critical area of transportation where a number of federal agencies and local stakeholders have taken many actions to secure seaports. Since the terrorist attacks of September 11, the nation's 361 seaports have been increasingly viewed as potential targets for future terrorist attacks. These ports are vulnerable because they are sprawling, interwoven with complex transportation networks, close to crowded metropolitan areas, and are easily accessible. Ports contain a number of specific facilities that could be targeted by terrorists, including military vessels and bases, cruise ships, passenger ferries, terminals, locks and dams, factories, office buildings, power plants, refineries, sports complexes, and other critical infrastructure. The large cargo volumes passing through seaports, such as containers destined for further shipment by other modes of transportation such as rail or truck, also represent a potential conduit for terrorists to smuggle weapons of mass destruction or other dangerous materials into the United States. The potential consequences of the risks created by these vulnerabilities are significant as the nation's economy relies on an expeditious flow of goods through seaports. Although no port-related terrorist attacks have occurred in the United States, terrorists overseas have demonstrated their ability to access and destroy infrastructure, assets, and lives in and around seaports. A successful attack on a seaport could result in a dramatic slowdown in the supply system, with consequences in the billions of dollars.

Much was set in motion to address these risks in the wake of the 9/11 terrorist attacks. We have reported that a number of actions have been taken or are under way to address seaport security by a diverse mix of agencies and seaport stakeholders. Federal agencies, such as the Coast Guard, CBP, and TSA, have been tasked with responsibilities and functions intended to make seaports more secure, such as monitoring vessel traffic or inspecting cargo and containers, and procuring new assets such as aircraft and cutters to conduct patrols and respond to threats. In addition to these federal agencies, seaport stakeholders in the private sector and at the state and local levels of government have taken actions to enhance the security of seaports, such as conducting security assessments of infrastructure and vessels operated within the seaports and developing security plans to protect against a terrorist attack. The actions taken by these agencies and stakeholders are primarily aimed at three types of protections: (1) identifying and reducing vulnerabilities of the facilities, infrastructure, and vessels operating in seaports; (2) securing the cargo and commerce flowing through seaports; and (3) developing greater maritime domain awareness through enhanced intelligence, information-sharing capabilities, and assets and technologies.

Our work indicated that assessments of potential targets have been completed at 55 of the nation's most economically and militarily strategic seaports, and more than 9,000 vessels and over 3,000 facilities have developed security plans that have been reviewed by the Coast Guard. New assets are budgeted and are coming on line, including new Coast Guard boats and cutters and communication systems. Finally, new information-sharing networks and command structures have been created to allow more coordinated responses and increased awareness of activities going on in the maritime domain. Some of these efforts have been completed and others are ongoing; overall, the amount of effort has been considerable. (Federal efforts to secure container cargo crossing U.S. borders by land or sea are discussed later in this report.) (See app. III for information on our products related to maritime security.)

## TSA and Other Agencies Have Begun Using a Risk-Management Approach to Identify and Prioritize Transportation Security Needs and Investments

Even with all the actions taken since 9/11 by Congress and federal agencies to strengthen our transportation-related layers of defense, we have reported that it seems improbable that all risk can be eliminated, or that any security framework can successfully anticipate and thwart every type of potential terrorist threat that highly motivated, well skilled, and adequately funded terrorist groups could devise. This is not to suggest that security efforts do not matter—they clearly do. However, it is important to keep in mind that total security cannot be bought no matter how much is spent on it. We cannot afford to protect everything against all threats—choices must be made about security priorities. Thus, great care needs to be taken to assign available resources to address the greatest risks, along with selecting those strategies that make the most efficient and effective use of resources.

One approach we have advocated to help ensure that resources are assigned and appropriate strategies are selected to address the greatest risks is through risk management—that is, defining and reducing risk. To help federal decision makers determine how to best allocate limited resources, we have advocated, the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) has recommended, and the subsequent Intelligence Reform and Terrorism Prevention Act of 2004 requires that a risk management approach be employed to guide security decision making.[59] We have concluded that without a risk management approach, there is limited assurance that programs designed to combat terrorism are properly prioritized and focused. A risk

---

[59]Pub. L. No. 108-458, 118 Stat. 3638.

management approach is a systematic process for analyzing threats and vulnerabilities, together with the criticality (that is, the relative importance) of the assets involved. This process consists of a series of analytical and managerial steps, basically sequential, that can be used to assess vulnerabilities, determine the criticality (that is, the relative importance) of the assets being considered, determine the threats to the assets, and assess alternatives for reducing the risks. Once these are assessed and identified, actions to improve security and reduce the risks can be chosen from the alternatives for implementation. To be effective, this process must be repeated when threats or conditions change to incorporate any new information to adjust and revise the assessments and actions.

In July 2005, in announcing his proposal for the reorganization of DHS, the Secretary of the Department of Homeland Security declared that as a core principle of the reorganization, the department must base its work on priorities driven by risk. DHS has also taken steps to implement a risk-based approach to assessing risks in various transportation modes. For example, TSA completed an air cargo strategic plan 3 years ago that outlined a threat-based, risk management approach to secure the air cargo system by, among other things, targeting elevated risk cargo for inspection. TSA also completed an updated cargo threat assessment in April 2005. However, we reported in November 2005 that TSA had not yet established a methodology and schedule for completing assessments of air cargo vulnerabilities and critical assets—two crucial elements of a risk-based management approach without which TSA may not be able to appropriately focus its resources on the most critical security needs. We recommended that TSA, among other things, complete its assessments of air cargo vulnerabilities and critical assets. (TSA has not provided any documentation to indicate that either the methodology or the schedule has since been completed.) By not yet fully evaluating the risks posed by terrorists to the air cargo transportation system through assessments of systemwide vulnerabilities and critical assets, including analyzing information on air cargo security breaches, TSA is limited in its ability to focus its resources on those air cargo vulnerabilities that represent the most critical security needs and assure Congress that existing funds are being spent in the most efficient and effective manner.

With respect to passenger rail, DHS's Office of Grants and Training (OGT) has developed and implemented a risk assessment methodology that it has used to complete risk assessments at rail facilities around the country. As we reported in September 2005, rail operators we interviewed stated that OGT's risk management approach has helped them to allocate and

prioritize resources to protect their systems. OGT has provided over $320 million in grants to rail transit agencies for certain security activities since fiscal year 2003. OGT has also leveraged its grant-making authority to promote risk-based funding decisions for passenger rail by requiring, for example, that operators complete a risk assessment to be eligible for a transit security grant. TSA has also recently begun to conduct risk assessments of the rail sector as part of a broader effort to assess risk to all transportation modes, but has not completed these efforts or determined how to analyze and characterize risks that are identified. Until these efforts are completed, TSA will not be able to prioritize passenger rail assets based on risk and help guide investment decisions about protecting them. We recommended in 2005 that TSA establish a plan and time line for completing its methodology for conducting risk assessments and evaluate whether the risk assessments used by OGT should be leveraged to facilitate the completion of risk assessments for rail and other transportation modes.

Progress also has been made to analyze risks to other transportation sectors. For example, with respect to seaports, Coast Guard has been using a port security risk assessment tool for determining the risk associated with specific attack scenarios against key infrastructure or vessels in local ports. Under this approach, seaport infrastructure that is determined to be both a critical asset and a likely and vulnerable target would be a high priority for security enhancements or funding. In general, we have reported that the most progress has been made on fundamental steps, such as conducting risk assessments of individual assets, and that the least amount of progress has been made on developing ways to translate this information into comparisons and priorities across ports or across infrastructure sectors.[60]

## Federal Agencies Have Recognized the Need to Enhance Cooperation with Domestic and International Stakeholders in Order to Strengthen Transportation Security

Federal agencies with transportation security responsibilities should not expect to develop or implement enhanced security goals and standards for transportation without participation and input from other federal partners, as well as key state, local, private-sector, and international stakeholders. These stakeholders include, for example, federal transportation modal administrations such as FTA and FRA, local governments, air carriers and airports, rail and seaport operators, private industry trade associations,

---

[60]GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91 (Washington, D.C.: Dec. 15, 2005).

and foreign governments. It is important that all these stakeholders be involved, as applicable and appropriate, in coordinating security-related priorities and activities, and reviewing and sharing best practices on security-related programs and policies as a means of developing common security frameworks. Such efforts are important in part because we are increasingly interdependent when it comes to addressing security gaps. For example, we place Federal Air Marshals on international flights, and we match information from passengers on international flights bound for the United States against terrorist watch lists. This interdependence requires close coordination and opportunities to harmonize security standards and practices with critical stakeholders, such as foreign governments.

Federal partnerships with various domestic stakeholders are under way throughout the transportation sector. In aviation, for example, TSA has been developing partnerships with private air carriers to conduct passenger prescreening, but continues to face challenges both identifying and supporting the roles it expects air carriers to play in the prescreening process, especially with regard to Secure Flight. In making recommendations to TSA on passenger prescreening, we have emphasized the need for TSA to continue to strengthen federal partnerships, and its partnerships with air carriers, in order to coordinate passenger screening programs, such as Secure Flight. For passenger rail, as mentioned previously, we have also recommended that TSA collaborate with the Department of Transportation and private industry rail operators on developing security standards that reflect industry best practices. In response, TSA is taking action to strengthen its partnerships with these stakeholders and is currently working with the American Public Transportation Association on developing passenger rail security standards based upon best practices.

Establishing federal partnerships with foreign governments and industry associations tackling similar transportation security challenges can provide important strategic opportunities to learn about security practices and programs that have worked elsewhere. As European Union countries and others throughout the world become more focused on aviation and transportation security, and with the establishment of international aviation security standards, TSA officials have acknowledged the importance of coordinating and collaborating with foreign countries on security matters. We have ongoing work examining TSA's efforts to coordinate with foreign governments on aviation security and expect to report on our results in the first quarter of 2007.

In our work on passenger rail security, we identified some practices that are utilized abroad that U.S. rail operators or the federal government had not studied in terms of the feasibility, costs, and benefits. For example, covert testing to determine whether security personnel comply with established security standards, which has been conducted at rail stations in the United Kingdom and elsewhere, is one approach TSA and rail industry stakeholders could consider. We recommended, among other things, that TSA evaluate the potential benefits and applicability—as risk analyses warrant and as opportunities permit—of implementing covert testing processes and other security practices that were not currently in use in the United States at the time our September 2005 report. In response, TSA, through DHS, stated that it had been working with foreign counterparts on rail and transit security issues in order to share and glean best practices and intended to continue to do so.

## GAO Concluding Observations—Enhancing Security of Other Transportation Modes

It is understandable that in the months and years following the 9/11 attacks, Congress and federal departments focused primarily on meeting the aviation security deadlines contained in ATSA and, in general, addressing the aviation-related vulnerabilities exploited by the terrorists. Over time, recognizing the threats and vulnerabilities facing other transportation modes, TSA and other agencies have begun to address other transportation security needs that were not the focal point of 9/11, including passenger rail, the maritime sector, and surface transportation modes. In these areas, TSA and other agencies have begun to identify and set priorities, based on risk and other factors, in order to allocate finite resources to enhance protection of the nation's passenger rail systems, seaports, highways, and other critical transportation assets. Agencies have made some progress but have a long way to go toward working with domestic and international partners to identify critical transportation assets, develop strategies for protecting them, and use a risk-based approach to prioritize and allocate resources across competing transportation security requirements.

## Measures to Improve Visa Applicant Screening, Consular Counterterrorism Training, and Fraud Detection Have Strengthened the Visa Process as an Antiterrorism Tool

The visa process is a first layer of border security to prevent terrorists or criminals from gaining entry into the United States. Citizens of other countries seeking to enter the country temporarily for business and other reasons generally must apply for and obtain a visa. Before 9/11, U.S. visa operations focused primarily on illegal immigration concerns; after the attacks, greater emphasis was placed on using the visa process as a counterterrorism tool. Congress, DHS, and State have taken numerous actions to help strengthen the visa process by, among other things, expanding the name-check system used to screen applicants (including portions of the consolidated watch list), requiring in-person interviews for nearly all applicants, revamping consular training to focus on counterterrorism, and augmenting staff at consular posts. Steps also have been taken to help detect and prevent visa fraud. In addition, State and DHS officials have acknowledged that immigrant visa processes—whereby immigrants seeking permanent residency in the United States must obtain a certain type of visa—may warrant further review because these visa types could also pose potential security risks.

### Visa Process Prior to 9/11 Did Not Focus on Counterterrorism

Citizens of other countries seeking to enter the United States temporarily for business and other reasons generally must apply for and obtain a U.S. travel document, called a visa, at U.S. embassies or consulates abroad before arriving at U.S. ports of entry. The main steps required to obtain a visa are generally the same before and after 9/11: visa applicants must submit an application to a consulate or embassy; consular officials review the applicant's documentation; the applicant's information is checked against a name-check system maintained by State; officials then issue, or decline to issue, a visa, which the applicant may then present to CBP officials (formerly Immigration and Naturalization Service inspectors) for inspection prior to entering the United States.[61]

While the general visa process has remained intact, the focus before 9/11 was primarily on screening applicants to determine whether they intended to work or reside illegally in the United States, though screening for terrorists was also part of this process. The 9/11 Commission staff reported that no U.S. agency at the time of the attacks thought of the visa process as an antiterrorism tool, and noted that consular officers were not

---

[61]Since 2004, in-person interviews are also required for applicants with certain exceptions.

trained to screen for terrorists.[62] Overseas consular posts, which administer the visa process, were encouraged to promote international travel, and were given substantial discretion in determining the level of scrutiny applied to visa applications. For example, posts had latitude to routinely waive in-person interviews as part of their overall visa applicant screening process. In making decisions about who should receive a visa, consular officials relied on a State Department name-check database[63] that incorporated information from many agencies on individuals who had been refused visas in the past, had other immigration violations, and had raised terrorism concerns. This name-check database was the primary basis for identifying potential terrorists and other ineligible applicants.

With these policies and State's name-check system in place, the 19 hijackers exploited this process and were able to obtain visas. (See app. I for details on the hijackers' visa applications and a time line of visas issued to hijackers during this period.) Specifically, the hijackers were issued a total of 23 visas at five different consular posts from April 1997 through June 2001 (multiple visas were issued over this period, for different stays). These visas were issued based on the belief that the applicants were "good cases," that is, they were not perceived as security risks and were thought likely to return to their country at the end of their allotted time in the United States. For citizens of either Saudi Arabia or United Arab Emirates, for example, post policies were to consider all of these citizens as "good cases" for visas. Thus, it was policy for consular officers in these countries to issue visas to most Saudi and Emirati applicants without interviewing them unless their names showed up in the name-check database or they had indicated on their applications that they had a criminal history. In addition, consular managers at these posts said that the posts had accepted applications from Saudi and Emirati nationals that weren't completely filled out and lacked supporting documentation.

As it turned out, 17 of the 19 hijackers were citizens of either Saudi Arabia or United Arab Emirates. None of the visa applications for which we were

able to obtain documentation[64] was completely filled out and consular officers granted visas to all but 2 of the 15 hijackers for whom records were available, without conducting an interview. Moreover, while consular officers who issued visas to the hijackers followed established procedures for checking to see if these individuals were included in the name-check database when they applied for visas, the database did not contain information on any of them. While the intelligence community notified State a few weeks prior to 9/11 that it had identified two of them as possible terrorists who should not receive visas, the visas had already been issued—and although they were subsequently revoked, by that time the hijackers had entered the country.

## New Visa-Related Policies and Programs Have Been Implemented to Enhance Visa Security, Improve Applicant Screening, Prevent Fraud, and More

As we reported in September 2005, State, DHS, and other agencies have taken many steps since the 9/11 attacks to strengthen the visa process as an antiterrorism tool.[65] For example, the consular name-check database has been expanded—the information in this database now draws upon a subset of the Terrorist Screening Center's consolidated watch list as well as other information. Specifically, State, in cooperation with other federal agencies, has increased the amount of information available to consular officers in the name-check database by fivefold—from 48,000 records in September 2001 to approximately 260,000 records in June 2005. An additional 8 million records on criminal history from the FBI also are now available for the name-check process. In addition, under the leadership of the Assistant Secretary of State for Consular Affairs, our work shows that consular officers are receiving clear guidance on the importance of security as the first priority of the visa process. Our observations of consular sections at eight posts in 2005 confirmed, for instance, that consular officers overseas regard security as their top priority, while also recognizing the importance of facilitating legitimate travel to the United States.

### New Operating Procedures and Requirements Strengthen the Visa Issuance Process

Many new policies have been introduced, and existing policies revised, both to strengthen the visa process as a terrorist screening tool and to build in more structure for posts that have traditionally had discretionary

---

[64]We could not review the visa applications for 2 of 17 Saudi and Emirati hijackers because the posts had destroyed them in accordance with State's document destruction policies in effect at that time.

[65]GAO, *Border Security: Strengthened Visa Process Would Benefit from Improvements in Staffing and Information Sharing*, GAO-05-859 (Washington, D.C.: Sept. 13, 2005).

latitude in handling visa matters. One key policy change, mandated in the Intelligence Reform and Terrorism Prevention Act of 2004[66] and which we had previously recommended,[67] requires that consular posts conduct in-person interviews with most applicants for nonimmigrant visas with certain exceptions. Generally, applicants between the ages of 14 and 79 must submit to an in-person interview though under certain circumstances such interviews can be waived. To ensure that these and other new policies for strengthening the visa process as an antiterrorism tool would be understood and implemented by all consular officers at all posts, State, in consultation with DHS, has issued more than 80 new standard operating procedures related to security and other matters. For example, State has issued procedures implementing the legislative provision that places restrictions on the issuance of nonimmigrant visas to persons coming from countries that sponsor terrorism.[68] Another new procedure informs consular offices about fingerprint requirements for visa applicants.[69]

State has also established management controls to ensure that visa applications are processed in a consistent manner at each post, in part to reinforce security-related policies and procedures. For example, the department created Consular Management Assistance Teams to conduct management reviews and field visits of consular sections worldwide, providing guidance to posts on standard operating procedures. Over 90 of these reviews have been conducted, in which the teams evaluate operations and make recommendations to mitigate a range of potential vulnerabilities they identify in their visits.

---

[66]Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No, 108-458, 118 Stat. 3638, § 5301.

[67]We recommended to State in 2002 that more comprehensive risk-based guidelines on standards for how consular officers use the visa process to screen against potential terrorists, including the degree of discretion for waived interviews, among other things.

[68]Section 306 of the Enhanced Border Security and Visa Entry Reform Act of 2002 restricts the issuance of nonimmigrant visas to any alien from a country that is a state sponsor of international terrorism unless the Secretary of State determines the alien does not pose a safety or security threat. Currently, citizens from Cuba, Iran, Libya, North Korea, Sudan, and Syria must, under this provision, undergo security clearances from agencies in Washington, D.C., prior to adjudication by a consular officer.

[69]Consular officers are required to use biometric information to confirm the identity of most foreign nationals by scanning the right and left index fingers. Fingerprint scans must be cleared through DHS's Automated Biometric Identification System before an applicant can receive a visa.

In addition, as a means of adding a layer of security review prior to issuing new visas, DHS has, as directed by Congress,[70] assigned visa security officers in Saudi Arabia to review all visa applications prior to adjudication by State's consular officers, and to provide expert advice and training to consular officers on visa security at selected U.S. embassies and consulates. This effort, known as the Visa Security Program, is being expanded to other posts. According to State's consular officers, the deputy chief of mission, and DHS officials in Saudi Arabia, the visa security officers deployed in Riyadh and Jeddah, Saudi Arabia, strengthen visa security because of their law enforcement and immigration experience, as well as their ability to access and use information from law enforcement databases not immediately available, by law, to consular officers. Based on recommendations we made in 2005, DHS has developed performance data to assess the results of this program at each post.

## Consular Training on Counterterrorism and Security Supports State Department Efforts to Use Visa Application Process as Antiterrorism Tool

Consular officers' training has been revamped and expanded to emphasize counterterrorism. For example, the basic consular training course has been lengthened from 26 days to 31 days to provide added emphasis on visa security, counterterrorism awareness, and interviewing techniques. And last year, State initiated training to enhance interviewing techniques, specifically designed to help consular officers spot inconsistencies in a visa applicant's story or in the applicant's demeanor; such observations may form a sufficient basis for denying a visa. State Department officials believe this training is important to help consular officers determine, during the interview period, whether applicants whose documents do not indicate any terrorist ties show signs of deception.

## Visa Fraud-prevention Measures Implemented to Complement Other Counter-Terrorism Efforts

To complement efforts taken to implement new guidance, policies and procedures, and management controls, State also has taken actions to address the potential for visa fraud at consular posts. As the 9/11 Commission staff noted, 2 of the 19 terrorist hijackers used passports that had been manipulated in a fraudulent manner to obtain visas needed to enter the country. State has since deployed 25 visa fraud investigators to U.S. embassies and consulates and developed ways for consular officers in the field to learn about fraud prevention including, for example, an on-line discussion group, comprised of more than 500 members, where information on, and lessons learned from, prior fraud cases may be shared. Training on fraud prevention also has been bolstered. For example, State expanded fraud prevention course offerings for managers

---

[70]Pub. L. No. 107-296, §428(e) and 428(i).

from 2 to 10 times annually; DHS's ICE provides training to State's fraud prevention managers; and ICE's Forensic Document Laboratory provides training on forensic documentation and analysis to combat travel and identity document fraud.

Acting on a recommendation we made in 2005 on fraud prevention, State's Vulnerability Assessment Unit[71] has begun to conduct more in-depth analyses of the visa information that is collected as a means of detecting patterns and trends that may indicate the potential for fraud and determining whether additional investigation may be needed. Using data-mining techniques (searching large volumes of data for patterns), this unit can, for example, use its internal databases to trigger alerts when specific keywords or activities arise, such as visas issued to individuals associated with certain organizations with terrorist ties, or sudden increases in visas issued to individuals residing in countries where they are not citizens. This proactive analysis may result in investigations and further mitigates potential fraud risks in the visa process.

In addition, the Intelligence Reform and Terrorist Prevention Act of 2004 required State in coordination with DHS to conduct a survey of each diplomatic and consular post to assess the extent to which fraudulent documents are presented by visa applicants.[72] The act mandates that State in coordination with DHS identify the posts experiencing the greatest frequency of fraudulent documents being presented by visa applicants and place in those posts at least one full-time antifraud specialist. The presence of full-time fraud officers at high-fraud posts is particularly important given that entry-level officers may serve as fraud prevention managers on a part-time basis, in addition to their other responsibilities.[73] According to State officials, as of July 2006, State had completed its review of fraud levels at posts, and is continuing to refine its methodology for determining which posts have the highest levels of fraud in the visa process.

---

[71]The Vulnerability Assessment Unit, staffed with personnel from the Bureau of Consular Affairs and Diplomatic Security, is responsible for analyzing consular data to identify anomalies related to internal fraud, such as visa issuances occurring during non-work hours. In response to our recommendation, the unit has expanded its work to encompass external fraud prevention.

[72]Pub. L. No. 108-458, §7203, 118 Stat. 3638.

[73]Consular officers who serve as fraud prevention managers are in charge of investigating cases of fraud, conducting fraud training for the consular section, and providing information on fraud relevant to the consular section at post.

## State Is Addressing Consular Staffing and Language-Proficiency Challenges

In addition to implementing new policies, procedures, and antifraud measures, State also has taken some steps to address staffing and language proficiency issues at consular posts. Though State added hundreds of Foreign Service consular positions after 9/11, and an additional 150 consular officer positions have been authorized annually from fiscal year 2006 through fiscal year 2009, State has reported that a staffing shortage at consular posts persists, and we have reported on multiple occasions that State has a shortage of mid-level, supervisory, consular officers at key overseas posts, and that the department has not assessed its overall consular staffing needs. Staff shortages have also led to extensive wait times for visa interview appointments at some posts. We are currently reviewing this issue and expect to report on our findings early this year. Moreover, in our earlier work, we found that not all consular officers were proficient in languages at their posts in order to hold interviews with visa applicants.[74] To remedy a shortage of consular officers able to speak critical languages, State has made efforts to focus recruitment of consular officers to include more who are proficient in languages it deems critical. (See app. III for a list of our products related to the visa process.)

## Potential Security Risks of Visa Programs for Immigrants Seeking Permanent Residency Status Warrant Review

While State and other agencies have enhanced and strengthened policies and procedures for screening applicants for nonimmigrant visas, State and DHS have acknowledged that the visa process for immigrants seeking to reside in the United States on a permanent basis may warrant further review because these visa types could also pose potential security risks. Immigrant visas are issued on the basis of certain family relationships or types of employment, refugee status, or other circumstances adjudicated by officials at several federal agencies, including the departments of Homeland Security, Labor, and Justice. We have recently begun a review to identify the security risks associated with various immigrant visa programs, and plan to issue a report later this year.

One immigrant visa program singled out by the State OIG 3 years ago as potentially risky was the Diversity Visa program, established by Congress in 1995. It authorizes the issuance of up to 50,000 immigrant visas annually to persons from countries that are underrepresented among the 400,000 to 500,000 immigrants coming to the United States each year, and who qualify

---

[74]See GAO-03-132NI.

for a visa on the basis of their education level and/or work experience.[75] This program is commonly referred to as the visa lottery because "winners" are selected through a computer-generated random drawing.[76] The applicants who receive a visa under this program are authorized to live and work permanently in the United States. The State OIG reported as a concern in 2003 that the Diversity Visa program did not generally prohibit the issuance of visas to aliens from countries that sponsor terrorism. (The nonimmigrant visa process, by contrast, places restrictions on the issuance of visas to persons from countries sponsoring terrorism.) Steps have since been taken by the State Department to address this concern. In 2005, the OIG reported that revised consular procedures and heightened awareness generally provided greater safeguards against terrorists entering through the Diversity Visa process than in the past. For example, the OIG noted that consular officers interview all Diversity Visa winners and check applicants' police and medical records. In addition, all immigrant visa applicants (as well as nonimmigrant applicants) are required to be fingerprinted; the fingerprint system helps to identify fraudulent applicants using false names. Despite these actions, the OIG continues to believe that the program still poses significant risks to national security from hostile intelligence officers, criminals, and terrorists attempting to use the program for entry into the United States as permanent residents. We are also reviewing the potential security risks of the Diversity Visa program as part of our ongoing review of immigrant visa programs.

## GAO Concluding Observations—Visa Process

The range of actions that State and DHS have undertaken to strengthen the nonimmigrant visa process as an antiterrorism tool—in part in response to our past recommendations---have, when considered altogether, gone a long way toward reducing the likelihood that terrorists can obtain the visas needed to enter the United States and wreak havoc. While it is generally acknowledged that the visa process can never be entirely failsafe—and that it will never be possible to entirely eliminate the risk of terrorists obtaining nonimmigrant visas issued by the United States government—the federal government has done a creditable job overall of

---

[75]Most immigrants entering the United States who do not participate in this program enter on the basis of family relationships or employment.

[76]Those selected are, like other visa applicants, subject to all grounds of ineligibility related to adverse medical conditions, criminal behavior, and other factors. If deemed eligible on those grounds, they need only to demonstrate that they have the equivalent of a U.S. high school education or possess 2 years of work experience in an occupation that requires at least 2 years of training or experience.

strengthening the visa process as a first line of defense. Separate concerns have been raised about potential risks associated with certain immigrant visa programs, and we have initiated a review to identify and analyze these potential security risks.

# Efforts to Screen and Verify Travelers and Detect Fraudulent Travel Documents Have Enhanced Border Security, but We Have Reported More Work Is Needed to Ensure That Risks Posed by Certain Travelers and Cargo Are Mitigated

The processes for screening and inspecting travelers arriving at the nation's air, land, and sea ports represent a key layer of border security defense. Many measures have been put in place to enhance security in these and related areas, but policies and programs can still be strengthened. For example, the Visa Waiver Program, which enables travelers from certain countries to seek entry into the United States without visas, carries inherent security, law enforcement, and illegal immigration risks because, among other things, visa waiver travelers are not subject to the same degree of screening as those travelers required to obtain visas. In addition, the potential misuse of lost or stolen passports from visa waiver countries is a serious security problem that terrorists and others can potentially exploit. Since 9/11, in response to congressional requirements, DHS has begun taking steps designed to mitigate the risks posed by visa waiver travelers; however, we have reported that additional actions are needed to further mitigate the risks posed by the use of fraudulent identity documentation, including actions to ensure that foreign governments report information on lost or stolen passports. Separately, a border security initiative designed to verify travelers' identities—US-VISIT—has helped to process and authenticate travelers seeking entry (or reentry) to the country. A key goal of US-VISIT—tracking those who overstay their authorized stay—cannot be fully implemented, however, because, among other things, the exit portion of the initiative has not been developed. Steps also have been taken by various federal agencies to enhance detection of hazardous cargo shipped over land and to identify oceangoing cargo containers that also may contain hazardous materials or weapons, but more work is needed in both areas.

## The Government Faces Challenges in Assessing and Mitigating the Inherent Security Risks of the Visa Waiver Program

While significant progress has been made to ensure that terrorists do not obtain visas as a prelude to gaining entry to the United States, visa holders are by no means the only foreign travelers coming to the United States. Under the Visa Waiver Program, millions of travelers seek entry into the United States each year without visas. The Visa Waiver Program is intended to facilitate international travel and commerce, and ease consular workload at overseas posts, by enabling citizens of 27 participating countries to travel to the United States for tourism or business for 90 days or less without first obtaining a nonimmigrant visa

from U.S. embassies and consulates.[77] (See app. II for a map of Visa Waiver Program member countries.) While the Visa Waiver Program provides many benefits to the United States, there are inherent security, law enforcement, and illegal immigration risks in the program because some foreign citizens may exploit the program to enter the United States. In particular, visa waiver travelers are not subject to the same degree of screening as those travelers who must first obtain a visa before arriving in the United States. Furthermore, lost and stolen passports from visa waiver countries could be used by terrorists, criminals, and immigration law violators to gain entry into the United States. While DHS established a unit in 2004 to oversee the program and conduct mandated assessments of program risks, we reported in July 2006 that the assessment process has weaknesses and the unit was unable to effectively monitor risks on a continuing basis because of insufficient resources.[78] Furthermore, while DHS has taken some actions to mitigate program risks, the department has faced difficulties in further mitigating the risks of the program, particularly regarding lost and stolen passports—a key vulnerability.

## Visa Waiver Travelers and Visa Applicants Face Different Levels of Screening, by Design

In fiscal year 2005, nearly 16 million travelers entered the United States under the Visa Waiver Program, and visa waiver travelers have represented roughly one-half of all nonimmigrant admissions to the United States in recent years. The program is beneficial, according to federal officials, because it facilitates international travel for millions of foreign citizens seeking to visit the United States each year, provides reciprocal visa-free travel for Americans visiting visa waiver member countries, and creates substantial economic benefits for the United States. Moreover, the program allows State to allocate its limited resources to visa-issuing posts in countries with higher-risk applicant pools.

By design, visa waiver travelers are not subject to the same degree of screening as those travelers who must first obtain a visa before arriving in

---

[77]The participating countries 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 United Kingdom. Participating countries were selected because, among other things, their citizens demonstrated a pattern of compliance with U.S. immigrant laws. Under certain circumstances, citizens of Canada and Bermuda may also travel to the United States without obtaining a visa, though they are not Visa Waiver Program members.

[78]GAO, *Border Security: Stronger Actions Needed to Assess and Mitigate Risks of the Visa Waiver Program*, GAO-06-854 (Washington, D.C.: July 28, 2006).
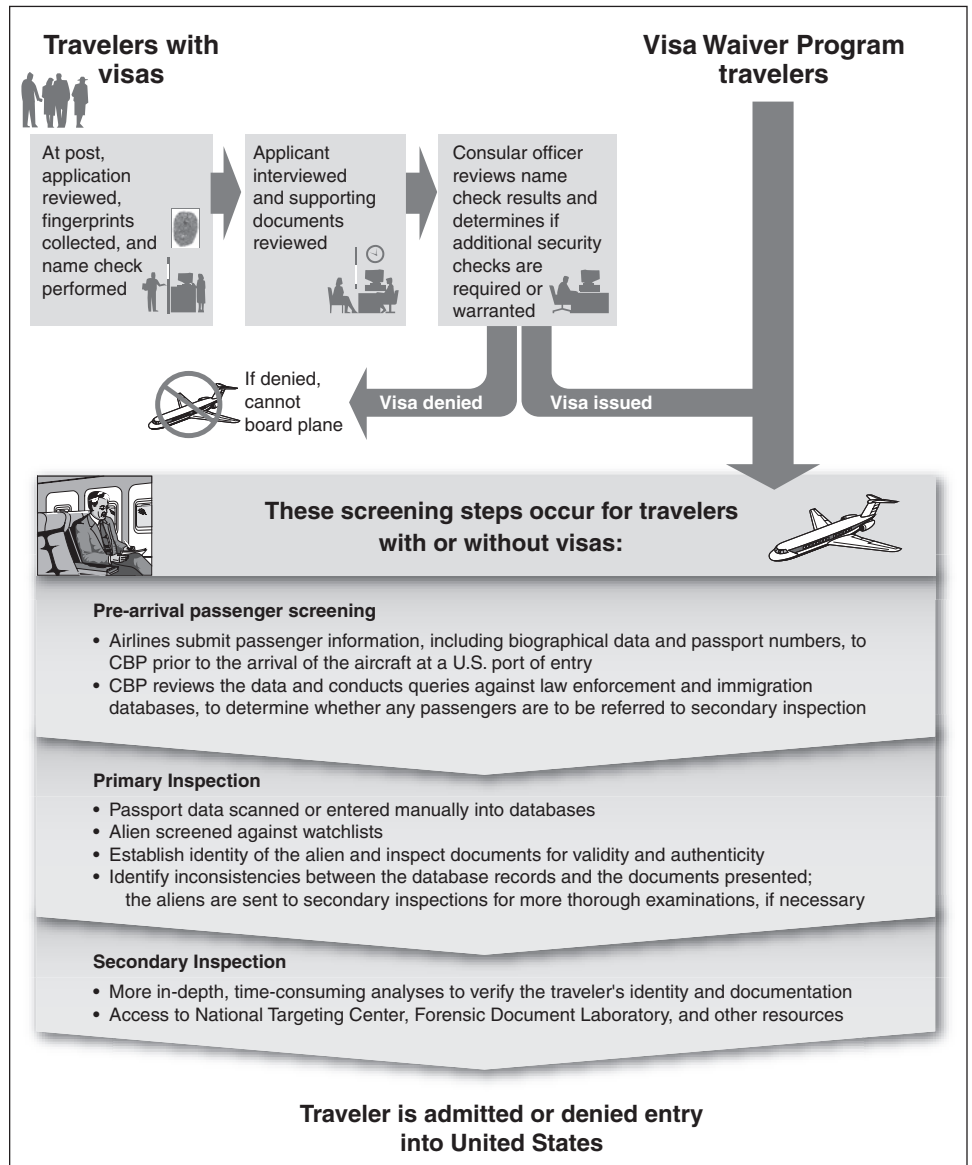
the United States. Travelers who must apply for visas receive two levels of screening as they are first screened by consular officers overseas and then by CBP officers before entering the country. However, visa waiver travelers are first screened in person by a CBP inspector upon arrival at a U.S. port of entry.[79]

For all travelers, CBP primary officers observe the applicant, examine that person's passport, collect the applicant's fingerprints as part of the U.S. Visitor and Immigrant Status Indicator Technology program (US-VISIT), and check the person's name against automated databases and watch lists, which contain information regarding the admissibility of aliens, including known terrorists, criminals, and immigration law violators. However, according to the DHS Office of Inspector General, CBP's primary border officers are disadvantaged when screening visa waiver travelers because they may not know the alien's language or local fraud trends in the alien's home country, nor have the time to conduct an extensive interview. In contrast, non-visa waiver travelers, who must obtain a visa from a U.S. embassy or consulate, undergo an interview by consular officials overseas, who conduct a rigorous screening process when deciding to approve or deny a visa. Moreover, consular officers have more time to interview applicants and examine the authenticity of their passports, and may speak the visa applicant's native language, according to consular officials. Fig. 5 provides a comparison of the process for visa waiver travelers and visa applicants.

---

[79]All foreign visitors, whether they have visas or are seeking to enter the United States under the Visa Waiver Program, undergo inspections by CBP officers at U.S. air, sea, and land ports of entry to ensure that only admissible persons enter the United States.

**GAO-07-375 Progress to Address Security After 9/11**

**Figure 5: Traveler Screening Process: U.S. Visa Holders versus Visa Waiver Program Travelers**

**Travelers with visas**

**Visa Waiver Program travelers**

At post, application reviewed, fingerprints collected, and name check performed

Applicant interviewed and supporting documents reviewed

Consular officer reviews name check results and determines if additional security checks are required or warranted

If denied, cannot board plane

**Visa denied**

**Visa issued**

**These screening steps occur for travelers with or without visas:**

**Pre-arrival passenger screening**
- Airlines submit passenger information, including biographical data and passport numbers, to CBP prior to the arrival of the aircraft at a U.S. port of entry
- CBP reviews the data and conducts queries against law enforcement and immigration databases, to determine whether any passengers are to be referred to secondary inspection

**Primary Inspection**
- Passport data scanned or entered manually into databases
- Alien screened against watchlists
- Establish identity of the alien and inspect documents for validity and authenticity
- Identify inconsistencies between the database records and the documents presented; the aliens are sent to secondary inspections for more thorough examinations, if necessary

**Secondary Inspection**
- More in-depth, time-consuming analyses to verify the traveler's identity and documentation
- Access to National Targeting Center, Forensic Document Laboratory, and other resources

**Traveler is admitted or denied entry into United States**

Sources: GAO; Nova Development (clip art).

**DHS Has Taken Steps to Enhance Oversight of Visa Waiver Program Countries' Participation but There Are Weaknesses in Program Oversight**

The Visa Waiver Program, while valuable, can pose risks to U.S. security, law enforcement, and immigration interests because some foreign citizens may try to exploit the program to enter the United States. Indeed, convicted 9/11 terrorist Zacarias Moussaoui and "shoe-bomber" Richard Reid both boarded flights to the United States with passports issued by Visa Waiver Program countries. Moreover, as we have reported,[80] inadmissible travelers who need visas to enter the United States may attempt to acquire a passport from a Visa Waiver Program country to avoid the additional scrutiny that takes place in non-visa waiver countries. Since the terrorist attacks, the government has taken several actions intended to enhance the security of the Visa Waiver Program by improving program management, oversight, and efforts to assess and mitigate program risks, among other things. For example, shortly after 9/11, Congress required DHS to increase the frequency of mandated assessments to determine the effect of each country's continued participation in the Visa Waiver Program on U.S. security, law enforcement, and immigration interests, from once every 5 years to once every 2 years (biennially).[81] These assessments are important because they enable the United States to analyze individual participating countries' border controls, security over passports and national identity documents, and other matters relevant to law enforcement, immigration, and national security. In April 2004, the DHS OIG reported that a lack of funding, training and other issues left DHS unable to comply with the congressionally mandated biennial country assessments.[82] In response to the OIG's findings, DHS established a Visa Waiver Program Oversight Unit[83] to oversee Visa Waiver Program activities and monitor countries' adherence to the program's statutory requirements to help ensure that the United States is protected from those who wish to do it harm or violate its laws, including immigration laws. Actions taken by this unit include completing comprehensive assessments for 25 of the 27 visa waiver countries (with the remaining two under way); identifying

---

[80]See GAO-06-854.

[81]The Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173.

[82]Prior to the establishment of DHS in 2003, Justice's Office of the Inspector General also examined visa waiver operations in 1999 and 2001, when the then-Immigration and Naturalization Service managed the program. Justice's Inspector General identified several chronic and recurring problems and made a series of recommendations to strengthen the implementation of the program.

[83]The unit is within the Office of International Enforcement, located in the Office of Policy Development under the direction of the Assistant Secretary of Homeland Security for Policy.

risks through these assessments, which were brought to the attention of host country governments for five countries; working with countries seeking to join the program; and briefing foreign government representatives from participating countries on issues of interest and concern such as new passport requirements for visa waiver travelers.

While the move to a biennial review process and establishment of the Visa Waiver Program Oversight Unit represents a good first step to better assess the inherent risks of the program, our recent work indicates that DHS could improve its administration of this effort and raises concerns about the agency's ability to effectively monitor the law enforcement and security risks due to staffing and resource constraints. For example, in our July 2006 report, we identified several problems with DHS's first biennially based review cycle conducted in 2004, including the lack of clear criteria when assessing each country's participation in the program to determine at what point security concerns in a particular country would trigger discussions with foreign governments to resolve them. Moreover, DHS did not issue the mandated summary report to Congress in a timely manner, describing the findings from its 25 country assessments. DHS, State, and Justice officials acknowledged that the report—consisting of a six-page summary lacking detailed descriptions of the law enforcement and security risks identified during the review process and which was delivered more than a year after the site visits were made—took too long to complete. As a result of this lengthy process, the final report delivered to Congress did not necessarily reflect the current law enforcement and security risks posed by each country, and did not capture recent developments. For example, the large-scale theft of blank passports in a visa waiver country that took place while the report was being processed was not reflected in the country's report. Thus, there were missed opportunities to report timely information to Congress. In our July 2006 report, we recommended that DHS finalize clear, consistent, and transparent protocols for biennial country assessments and provide these protocols to stakeholders at relevant agencies at headquarters and overseas. These protocols should provide time lines for the entire assessment process, including the role of a site visit, an explanation of the clearance process, and deadlines for completion. In addition, we recommended to Congress that it establish a biennial deadline by which DHS must complete its assessments and report to Congress. In its formal comments to our report, DHS did not appear to support the establishment of a deadline. Instead, DHS suggested that Congress require continuous and ongoing evaluations of the risks of each country's program.

With respect to staffing and resources to carry out these assessment efforts and other program oversight responsibilities, we reported that DHS cannot effectively monitor the law enforcement and security risks posed by 27 visa waiver countries on a consistent, ongoing basis because it has not provided the oversight unit with adequate staffing and funding resources. Without adequate resources, the unit may be unable to monitor and assess participating countries' compliance with the program. We recommended that additional resources be provided to strengthen the program oversight unit's monitoring activities. Until this is achieved, staffing and resource constraints may hamper the effectiveness of the Visa Waiver Program and could jeopardize U.S. security interests.[84] DHS has stated that it expects the administration to seek resources appropriate for the oversight unit's tasks.

## Federal Agencies Have Begun to Address Security Risks Arising from Lost or Stolen Passports, but We Have Reported That Additional Actions are Needed to Further Mitigate These Risks

In addition to efforts to improve administration and oversight and assess the overall risks of the Visa Waiver Program, federal actions also have been taken to mitigate one specific risk: the potential misuse of lost or stolen passports. DHS intelligence analysts, law enforcement officials, and forensic document experts all acknowledge that the greatest security problem posed by the program is the potential exploitation by terrorists, immigration law violators, and other criminals of a country's lost or stolen passports—whether they've been issued (used) or are blank (unused). Lost and stolen passports from visa waiver countries are highly prized among those travelers seeking to conceal their true identities or nationalities. In 2004, the DHS OIG reported that aliens applying for admission to the United States using lost or stolen passports had little reason to fear being caught. DHS has acknowledged that an undetermined number of inadmissible aliens may have entered the United States using a stolen or lost passport from a visa waiver country, and, in fact, passports from Visa Waiver Program countries have been used illegally by travelers attempting to enter the United States. For example, in a 6-month period in 2005, DHS confiscated 298 fraudulent or altered passports at U.S. ports of entry, which had been issued by visa waiver countries. Visa waiver countries that do not consistently report the losses or thefts of their citizens' passports, or of blank passports, put the United States at greater risk of allowing inadmissible travelers to enter the county.

DHS has begun taking steps intended to help mitigate the risks related to lost and stolen passports. For example, in 2004, the DHS OIG reported that

---

[84]See GAO-06-854.

a lack of training hampered CBP border inspectors' ability to detect passport fraud among visa waiver travelers and recommended that CBP officers receive additional training in fraudulent document detection.[85] In response, DHS has doubled the time devoted to fraudulent document detection training for new officers from 1 day to 2 days, and provides additional courses for officers throughout their assignments at ports of entry.

Nevertheless, training officials said that fraudulent and counterfeit passports are extremely difficult to detect, even for the most experienced border officers. Congress and DHS have taken additional actions designed to mitigate this risk. For example, all passports issued to visa waiver travelers between October 26, 2005 and October 25, 2006, must contain a digital photograph printed in the document, and DHS is enforcing this requirement. For example, when Italy and France failed to meet the deadline for issuing new passports encoded with digital photographs, DHS began requiring citizens with noncompliant passports to obtain a visa before visiting the United States. In addition, passports issued to visa waiver travelers after October 25, 2006, must be electronic (e-passports).[86] E-passports aim to enhance the security of travel documents, making it more difficult for imposters or inadmissible aliens to misuse the passport to gain entry into the United States. Travelers with passports issued after the deadlines that do not meet these requirements are required to obtain a visa from a U.S. embassy or consulate overseas before departing for the United States. On October 26, 2006, DHS announced that 24 of the 27 Visa Waiver Program countries had met the deadline to begin issuing e-passports.[87]

While e-passports may help officers to identify fraudulent and counterfeit passports, because many passports issued from a visa waiver country

---

[85]GAO has also reported on inspections at land ports of entry. GAO, *Land Border Ports of Entry: Vulnerabilities and Inefficiencies in the Inspections Process,* GAO-03-1084R (Washington, D.C.: Aug. 18, 2003).

[86]In general, e-passports contain a chip, which is embedded in the passport. The chip stores the same information that is printed in the data page of the passport: the name, date of birth, gender, place of birth, dates of passport issuance and expiration, place of issuance, passport number, and photo image of the bearer. In addition, it holds the unique chip identification number and a digital signature to protect the stored data from alteration.

[87]According to DHS, the United States continues to work with the three countries— Andorra, Brunei, and Liechtenstein—that did not meet the deadline to ensure that they meet the requirement as soon as possible.

before the October 2006 deadline are not electronic—and remain valid for years to come—it remains imperative that lost and stolen passports from visa waiver countries be reported to the United States on a timely basis. In 2002, Congress made the timely reporting of stolen blank passports, in particular, a condition for continued participation in the program and required that a country must be terminated from the Visa Waiver Program if the Secretary of Homeland Security and the Secretary of State jointly determine that this information was not reported on a timely basis. According to DHS, detecting stolen blank passports at U.S. ports of entry is extremely difficult and some thefts of blank passports have not been reported to the United States until years after the fact. For example, in 2004, a visa waiver country reported to the United States the theft of nearly 300 blank passports more than 9 years after the theft occurred. DHS and State have chosen not to terminate from the program countries that failed to report these incidents. DHS officials told us that the inherent political, economic, and diplomatic implications associated with removing a country from the Visa Waiver Program make it difficult to enforce the statutory requirement. Nevertheless, recognizing the importance of timely reporting of this information, DHS has taken steps to address this issue. For example, in 2004, during its assessment of Germany's participation in the Visa Waiver Program, DHS determined that several thousand blank German temporary passports[88] had been lost or stolen, and that Germany had not reported some of this information to the United States. In response, after a series of diplomatic discussions, temporary passport holders from Germany were no longer allowed to travel to the United States without a visa. In addition, because lost or stolen issued passports can be altered, DHS issued guidance in 2005 to visa waiver countries requiring that they certify their intent to report lost or stolen passport data on issued passports. Some visa waiver countries do not provide this information to the United States, due in part to concerns over the privacy of their citizens' biographical information.

While we acknowledge the complexities and challenges of enforcing the statutory requirement and collecting information on both blank and issued stolen and lost passports aside, our recent work has identified areas where DHS could do more to help ensure that countries report this information—and do so in a timely manner. For example, as of June 2006, DHS had not

---

[88]German temporary passports are valid for one year, and are less expensive than standard German passports. In addition, they are issued at more than 6,000 locations in Germany, whereas the Ministry of Interior issues the standard passports centrally.

yet issued guidance or standard operating procedures on what information must be shared, with whom, and within what time frame. In July 2006, we recommended that DHS require all visa waiver countries to provide the United States with nonbiographical data from lost or stolen issued passports, as well as from blank passports, and develop and communicate clear standard operating procedures for the reporting of these data, including a definition of timely reporting and a designee to receive the information.[89]

In a separate effort to mitigate risks from lost and stolen passports, the U.S. government announced in 2005 its intention to require visa waiver countries to certify their intent to report information on lost and stolen blank and issued passports to the International Criminal Police Organization (Interpol)[90]—the world's largest international police organization. State reported to Congress in 2005 that it had instructed all U.S. embassies and consulates to take every opportunity to persuade host governments to share this data with Interpol. Interpol already has a database of lost and stolen travel documents to which its member countries may contribute on a voluntary basis. As of June 2006, this database contained more than 11 million records of lost and stolen passports. However, the way visa member countries and the United States interact with and utilize the Interpol database system could be improved. While most of the 27 visa waiver countries use and contribute to Interpol's database, 4 do not. Moreover, some countries that do contribute do not do so on a regular basis, according to Interpol officials. In addition, Interpol's data on lost and stolen travel documents are not automatically accessible to U.S. border officers at primary inspection—which is one reason why it is not an effective border screening tool, according to DHS, State, and Justice officials. According to the Secretary General of Interpol, until DHS can automatically query Interpol's data, the United States will not have an effective screening tool for checking passports. However, DHS has not yet finalized a plan to acquire this systematic access to Interpol's data. We recently recommended that DHS require all visa waiver countries to provide Interpol with nonbiographical data from lost or stolen issued or

---

[89]See GAO-06-854.

[90]Interpol is the world's largest international police organization, with 184 member countries. Created in 1923, it facilities cross-border police cooperation, and supports and assists all organizations, authorities, and services whose mission is to prevent or combat international crime. In July 2002, Interpol established a database on lost and stolen travel documents. As of June 2006, the database contained about 11.6 million records of lost and stolen passports.

blank passports, and implement a plan to make Interpol's database automatically available during primary inspection at U.S. ports of entry.

## GAO Concluding Observations—Visa Waiver Program

The Visa Waiver Program aims to facilitate international travel for millions of people each year and promote the effective use of government resources. Effective oversight of the program entails balancing these benefits against the program's potential risks. To find this balance, as we have reported, the U.S. government needs to fully identify the vulnerabilities posed by visa waiver travelers, and be in a position to mitigate them. However, we found weaknesses in the process by which the U.S. government assesses these risks, and DHS's Visa Waiver Program oversight unit is not able to manage the program with its current resource levels. While actions are under way to address these issues, they have not all been resolved. Specifically, in response to our recommendation that additional resources be provided to strengthen the program oversight unit's monitoring activities, DHS stated that it expected the administration to seek resources appropriate for the unit's tasks. Until this is achieved, as we have reported, staffing and resource constraints may hamper the effectiveness of the Visa Waiver Program and could jeopardize U.S. security interests. Moreover, DHS has not communicated clear reporting requirements for lost and stolen passports—a key risk—nor can it automatically access all stolen passport information when it is most needed—namely, at the primary inspection point at U.S. points of entry. We recently recommended that DHS require all visa waiver countries provide the United States and Interpol with nonbiographical data from lost or stolen issued passports, as well as from blank passports, and implement a plan to make Interpol's lost and stolen passport database automatically available during the primary inspection process at U.S. ports of entry. DHS is in the process of implementing these recommendations. Finding ways to address these and other challenges, including those related to program staffing and managing the visa waiver country review process, are especially important, given that, while it does not appear there will be any expansion of the Visa Waiver Program in the short term, many countries are actively seeking admission into the program, and the President has announced his support for the program's expansion.

## US-VISIT Border Security Initiative Helps to Process and Authenticate Travelers Entering the Country, but Identifying Overstays and Detecting Fraudulent Travel Documents Remain Challenges

Over the last decade, the United States has, at the direction of Congress, been developing a border security initiative intended to serve as a comprehensive system for recording the entry and exit of most foreign travelers. Prior to 9/11, this system, now known as US-VISIT, was the responsibility of the INS and focused primarily on trying to ensure that nonimmigrant travelers (including those from visa waiver countries) who arrived at U.S. ports of entry (POE)[91] did not overstay their authorized visitation periods in order to work illegally in the country. Our work in the years leading up to the 9/11 attacks, and work by the Justice Department OIG, found weaknesses in overstay processes, in part because the INS did not collect and maintain records that would enable officials to identify all of the foreign nationals who either left the country or who remained past the expiration date of their authorized stay. US-VISIT was initially conceived as one means of addressing this problem. After the terrorist attacks, while immigration enforcement remained an important priority, the ability to track overstays through an entry/exit border inspection system, and to authenticate the identity of travelers arriving at ports of entry, took on added importance, given that three of the six terrorist pilots had managed to remain in the U.S. after their visas had expired. In prior reports on US-VISIT, we have identified numerous challenges that DHS faces in delivering program capabilities and benefits on time and within budget. We have reported, for example, that the US-VISIT program is a risky endeavor, in part because it is large, complex, and potentially costly. (See app. III for a list of our products related to overstay tracking and US-VISIT.)

US-VISIT is designed to use biographic information (e.g., name, nationality, and date of birth) and biometric information (e.g., digital fingerprint scans) to verify the identity of those covered by the program, which is being rolled out over a 5-year period, from 2002 to 2007. The program applies to certain visitors whether they hold a nonimmigrant visa, or are traveling from a country that has a visa waiver agreement with the United States under the Visa Waiver Program. Foreign nationals subject to US-VISIT who intend to enter the country encounter different inspection processes at different types of ports of entry (POEs) depending on their mode of travel. Foreign nationals subject to US-VISIT who enter the United States at an air or sea POE are to be processed, for purposes of

[91]A port of entry is generally a physical location, such as a pedestrian walkway and/or a vehicle plaza with booths, and associated inspection and administration buildings, at a land border crossing point, or a restricted area inside an airport or seaport, where entry into the country by persons and cargo arriving by air, land, or sea is controlled by CBP.

US-VISIT, in the primary inspection area upon arrival. Generally, these visitors are subject to prescreening before they arrive via passenger manifests, which are forwarded to CBP by commercial air or sea carrier in advance of arrival.[92] By contrast, foreign nationals intending to enter the United States at a land POE are generally not subject to prescreening because they arrive in private vehicles or on foot and there is no manifest to record their pending arrival. Thus, when foreign nationals subject to US-VISIT arrive at a land POE, they are directed by CBP officers from the primary inspection area to the secondary inspection area for further processing.

As we have recently reported,[93] DHS has deployed an entry capability for US-VISIT at over 300 air, sea, and land POEs, including 154 land ports along the northern and southwestern borders where hundreds of millions of legitimate border crossings take place annually. Biographic and biometric information, including digital fingerprint scans and digital photographs, are used at these ports to verify the identity of visitors. With respect to land ports specifically (the subject of our most recent US-VISIT work), CBP officials at 21 land POE sites we visited where US-VISIT entry capability had been deployed reported that the program had enhanced their ability to verify travelers' identities, among other things. However, many land POE facilities, which are small and aging, face ongoing operational challenges, including space constraints and traffic congestion, as they continue to operate the entry capability of US-VISIT while also processing other travelers entering the United States. Moreover, Congress's goal for US-VISIT—to record entry, reentry, and exit—has not been fully achieved because a biometric exit capability has not been developed or deployed. According to DHS officials, implementing a biometrically-based exit program like that used to record those entering or re-entering the country is potentially costly (an estimated $3 billion), would require new infrastructure, and would produce major traffic congestion because travelers would have to stop their vehicles upon exit to be processed—an option officials consider unacceptable. Officials stated that they expect a viable technology for developing a biometric exit

---

[92]Under the Enhanced Border Security and Visa Entry Reform Act of 2002 (Pub. L. No. 107-173, § 402(a), 116 Stat. 543, 557-59), commercial air and sea carriers are to transmit crew and passenger manifests to appropriate immigration officials before arrival of an aircraft or vessel in the United States.

[93]GAO, *Homeland Security: Recommendations to Improve Management of Key Border Security Program Need to Be Implemented*, GAO-06-296 (Washington, D.C.: February 2006).

capability for US-VISIT that would not require travelers to stop at a facility will become available within the next 5 to 10 years. Without some type of biometric exit capability, however, the government cannot provide certainty that the person exiting the country is the person who entered—and thus cannot determine which visitors have remained in the U.S. past the expiration date of their authorized stay. In November 2006, we recommended, among other things, that DHS finalize a mandated report to Congress describing how a comprehensive biometrically based entry and exit system would work and how an interim nonbiometric exit solution—one is currently being tested—is to be developed or deployed.[94] DHS agreed with our recommendation.

While the goal of US-VISIT is in part to ensure that lawful travelers enter and exit the country using valid identity documents, the program is not intended to verify the identities of all travelers. In particular, U.S. citizens, lawful permanent residents, and most Canadian and Mexican citizens are exempt from being processed under US-VISIT upon entering and exiting the country. It is still possible for travelers such as these to use fraudulent documents as a basis for entering the country. For example, U.S. citizens and citizens of Canada and Bermuda are not generally required to present a passport when they enter the United States via land ports of entry. Instead, as we have reported, they may use other forms of identifying documentation, such as a driver's license or birth certificates, which can be easily counterfeited and used by terrorists to travel into and out of the country. In 2003, 2004, and again in 2006 our undercover investigators were able to successfully enter the United States from Canada and Mexico using fictitious names and counterfeit driver's licenses and birth certificates.

CBP officials have acknowledged that its officers are not able to identify all forms of counterfeit documentation of identity and citizenship presented at land ports of entry and the agency fully supports a new statutory initiative designed to address this vulnerability. This requires DHS and State to develop and implement a plan by no later than June 2009 whereby U.S. citizens and foreign nationals of Canada, Bermuda, and Mexico must present a passport or other document or combination of documents deemed sufficient to show identity and citizenship to enter or

---

[94]GAO, *Border Security: US-VISIT Program Faces Strategic, Operational and Technological Challenges at Land Ports of Entry*, GAO-07-56SU (Washington, D.C.: November 2006).

reenter the United States; such documentation is not currently needed by many of these travelers. While this effort, known as the Western Hemisphere Travel Initiative (WHTI),[95] may address concerns about counterfeit documents, it still faces hurdles. For example, key decisions have yet to be made about what documents other than a passport would be acceptable when U.S. and Canadian citizens enter or return to the United States via land ports of entry—a decision critical to making decisions about how DHS is to inspect individuals entering the country. Nor has DHS decided what types of security features should be utilized to protect personal information contained in travel documents that may be required, such as an alternative type of passport containing an electronic tag encoded with information to identify each traveler.[96] DHS also has not determined whether, or how, WHTI border inspection processes would fit strategically or operationally with other current and emerging border security initiatives.

The emergence of fraud-prevention efforts such as WHTI pose additional challenges for DHS's oversight of US-VISIT. For example, DHS has not yet determined how US-VISIT is to align with emerging land border security initiatives and mandates like WHTI, and thus cannot ensure that these programs work in harmony to meet mission goals and operate cost effectively. As we reported 3 years ago, agency programs need to properly fit within a common strategic context governing key aspects of program operations, such as what functions are to be performed and rules and standards governing the use of technology. Although a strategic plan defining an overall immigration and border management strategy has been drafted, DHS has not approved it, raising questions about DHS's overall strategy for effectively integrating border security programs and systems at land POEs. Until decisions about WHTI and other initiatives are made, it remains unclear how US-VISIT will be integrated with emerging border security initiatives, if at all—raising the possibility that CBP would be faced with managing differing technology platforms and border inspection processes at each land POE. Knowing how US-VISIT is to work in concert with other border security and homeland security initiatives could help Congress, DHS, and others better understand what resources and tools are

---

[95]See GAO-06-741R, *Observations on Efforts to Implement Western Hemisphere Travel Initiative on the U.S. Border with Canada* (Washington, D.C.: May 25, 2006).

[96]Since we reported our observations on efforts to implement WHTI, DHS and State have published *Federal Register* notices with proposed decisions in these areas, but final regulations have not been published.

needed to ensure their success. We recommended in November 2006 that DHS direct the US-VISIT Program Director to finalize in its required report to Congress (as noted earlier) a description of how DHS plans to align US-VISIT with other emerging land border security initiatives. DHS agreed with our recommendation. We have ongoing work looking at many aspects of US-VISIT.

## GAO Concluding Observations—US-VISIT

Developing and deploying complex technology that records the entry and exit of millions of visitors to the United States, verifies their identities to mitigate the likelihood that terrorists or criminals can enter or exit at will, and tracks persons who remain in the country longer than authorized is a worthy goal in our nation's effort to enhance border security in a post-9/11 era. But doing so also poses significant challenges; foremost among them is striking a reasonable balance between US-VISIT's goals of providing security to U.S. citizens and visitors while facilitating legitimate trade and travel. DHS has made considerable progress making the entry portion of the US-VISIT program at land ports of entry operational, and border officials have clearly expressed the benefits that US-VISIT technology and biometric identification tools have afforded them. With respect to DHS's effort to create an exit verification capability, developing and deploying this capability for US-VISIT at land POEs has posed a set of challenges that are distinct from those associated with entry. US-VISIT has not determined whether it can achieve, in a realistic time frame, or at an acceptable cost, the legislatively mandated capability to record the exit of travelers at land POEs using biometric technology. Finally, DHS has not articulated how US-VISIT fits strategically and operationally with other land-border security initiatives, such as the Western Hemisphere Travel Initiative and Secure Border Initiative. As we have recently reported, without knowing how US-VISIT is to be integrated within the larger strategic context governing DHS operations, DHS faces substantial risk that US-VISIT will not align or operate with other initiatives at land POEs and thus not cost-effectively meet mission needs. We recently recommended that DHS finalize a mandated report to Congress on US-VISIT that would include a description of how a comprehensive biometrically based entry and exit system would work and how DHS plans to align US-VISIT with other emerging land border security initiatives. DHS agreed with these recommendations.

## DHS Has Made Progress in Detecting Hazardous Materials and Cargo at Ports of Entry, but Security Challenges Remain

In addition to the challenges posed by travelers at U.S. ports of entry, various types of cargo also pose security challenges. Preventing radioactive material from being smuggled into the United States—perhaps to be used by terrorists in a nuclear weapon or in a radiological dispersal device (a so-called dirty bomb)—has become a key national security objective. DHS is responsible for providing radiation detection capabilities at U.S. ports of entry and implementing programs to combat nuclear smuggling. The departments of Energy, Defense, and State, are also implementing programs to combat nuclear smuggling in other countries by providing radiation detection equipment and training to foreign border security personnel. Our work in this area suggests that while the nation may always be vulnerable to some extent to this type of threat, DHS has improved its use of radiation detection equipment at U.S. ports of entry and is coordinating with other agencies to conduct radiation detection programs. DHS has, for example, improved in its use of radiation detection equipment and in following the agency's inspection procedures implemented since 2003.

We have nevertheless identified potential weaknesses in procedures for ensuring both that radioactive material is being obtained and used legitimately in the United States and that appropriate documentation, such as bills of lading, are provided when this material is transported across our borders. For example, we have conducted covert testing to determine whether it was possible to make several purchases of small quantities of radioactive material and used counterfeit documents to cross the border even if radiation monitors detected the radioactive sources we carried.[97] Our purchase of the radioactive substance was not challenged because suppliers are not required to determine whether a buyer has a legitimate use for the material. Nor are purchasers required to produce a document from the Nuclear Regulatory Commission when making purchases of small quantities. During our testing, the radiation monitors properly signaled the presence of radioactive material when our two teams conducted simultaneous border crossings and the vehicles were inspected. However, our investigators were able to enter the United States with the material because they used counterfeit documents. Specifically, the investigators were able to successfully represent themselves as employees of a fictitious company and present a counterfeit bill of lading and a counterfeit Nuclear

---

[97]GAO, *Border Security: Investigators Successfully Transported Radioactive Sources Across Our Nation's Borders at Selected Locations*, GAO-06-545R (Washington, D.C.: March 2006).

Regulatory Commission document during inspections. CBP officers never questioned the authenticity of our investigators' counterfeit documents. In response to our work, officials with the Nuclear Regulatory Commission told us that they are aware of the potential problems with counterfeit documentation and are working to resolve these issues.

In other work,[98] we have identified other potential weaknesses related to the regulation and inspection of radioactive materials being shipped to the United States. We found, for example, that while radiological materials being transported into the United States are generally required to have a Nuclear Regulatory Commission license, regulations do not require that the license accompany the shipment. Further, CBP officers do not have access to data that could be used to verify that shippers have acquired the necessary documentation. And CBP inspection procedures do not require officers to open containers and inspect them after an initial alarm is triggered, although under some circumstances, doing so could improve security. DHS has sponsored research, development, and testing activities to address the inherent limitations of currently fielded detection equipment. However, much work remains to achieve consistently better detection capabilities. We have recently recommended to DHS and CBP that, among other things, CBP's inspection procedures be revised to include physically opening cargo containers in certain circumstances where external inspections prove inconclusive and that federal officials find ways to authenticate licenses that accompany radiological shipments. DHS agreed with our recommendations and has committed to implementing them. (See app. III for a list of our products related to hazardous materials crossing our borders.)

In addition to the hazards posed by certain types of land-based cargo, government officials recognize that terrorism also poses risks to oceangoing cargo traveling to and from commercial U.S. seaports. Ocean cargo containers play a vital role in the movement of cargo between global trading partners. In 2004 alone, nearly 9 million ocean cargo containers arrived and were offloaded at U.S. seaports. Responding to heightened concern about national security since 9/11, several U.S. government agencies have focused efforts on preventing terrorists from smuggling weapons of mass destruction in cargo containers from overseas locations

---

[98]GAO, *Combating Nuclear Smuggling: DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports-of-Entry, but Concerns Remain*, GAO-06-389 (Washington, D.C.: March 2006).

to attack the United States and disrupt international trade. To help address its responsibility to ensure the security of this cargo, CBP has in place a program known as the Container Security Initiative. The program aims to target and inspect high-risk cargo shipments at foreign seaports before they leave for destinations in the United States. Under the program, foreign governments agree to allow CBP personnel to be stationed at foreign seaports to use intelligence and risk assessments to target shipments to identify those at risk of containing weapons of mass destruction or other terrorist contraband. As of February 2005 (the date of our most recent work),[99] the Container Security Initiative program was operational at 34 foreign seaports, with plans to expand to an additional 11 ports by the end of fiscal year 2005. We have advocated in recent testimony[100] that CBP's targeting system should, among other things, take steps to assess the risks posed by oceangoing cargo. (See app. III for a list of our products related to other cargo security initiatives.)

## GAO Concluding Observations—Border Security

Whether the security challenge facing federal authorities at ports of entry involves persons or cargo, the job of securing the nation's borders is daunting. The task involves the oversight and management of nearly 7,500 miles of land borders with Canada and Mexico, and hundreds of legal ports of entry through which millions of travelers are inspected annually. After 9/11, the government took immediate steps to tackle some of the major border-related vulnerabilities and challenges that we and others had identified, such as those related to passport and document fraud and tracking overstays. While it may never be possible to ensure that all terrorists, criminals, or those violating immigration laws are prevented from entering the country, DHS and other agencies must remain vigilant in developing and implementing programs and policies designed to reduce breaches in our borders and ensure that hazardous cargoes are interdicted.

[99]See Container Security: *A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts*, GAO-05-557 (Washington, D.C.: April 26, 2005).

[100]*Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve Automated Targeting Systems*, GAO-06-591T (Washington, D.C.: March 30, 2006).

**GAO-07-375 Progress to Address Security After 9/11**

## Federal Government Must Address Strategic Challenges of Sharing Terrorism-Related Information, Managing Risk, and Structuring DHS to Meet Its Mission

Five years after 9/11 and in the wake of new terrorist threats and tactics, Congress, DHS, and other federal agencies face an array of strategic challenges that potentially affect the ability of each to effectively oversee or execute the ambitious goals and programs that are under way or planned to enhance homeland security. U.S. leaders and policy makers continue to face the need to choose an appropriate course of action going forward—setting priorities, allocating resources, and assessing the social and economic costs of the measures that may be taken governmentwide to further strengthen domestic security. Balancing the trade-offs inherent in these choices—and aligning policies to support them—will not be easy, but is nonetheless essential. Accomplishing this critical task will be further challenged by (1) the federal government's continued struggle to share information needed to combat terrorism across federal departments and with state and local governments; (2) having to implement a system that assesses the relative risks reduced by investing scarce dollars among varied and competing security alternatives; and (3) a DHS that continues to struggle in becoming a fully integrated and effectively functioning organization that is prepared and positioned to successfully protect the homeland from future terrorist threats.

## Efforts to Share Critical Information on Terrorism Have Improved Since 9/11, but a Governmentwide Framework for Information Sharing Has Still Not Been Implemented

There are numerous challenges that cut across branches of the federal government that must be addressed broadly and in a coordinated fashion at the highest levels. One of the most important and conspicuous of these cross-cutting challenges involves the sharing of information related to terrorism. The former vice chairman of the 9/11 Commission identified the inability of federal agencies to effectively share information about suspected terrorists and their activities as the government's single greatest failure in the lead-up to the 9/11 attacks. As discussed earlier in this report, FAA's no-fly list only contained 12 names of potential terrorists on 9/11 because information collected by other agencies, such as the CIA and FBI about terrorist suspects was not shared with FAA at the time. According to the 9/11 report, this undistributed information would have helped identify some of the terrorists, but such information was shared only on a need-to-know rather than a need-to-share basis. The commission recommended, among other things, that terrorism-related information contained in agency databases should be shared across agency lines. Because of the significance of this issue, we designated information sharing for homeland security as a governmentwide high-risk area in 2005.

Responding to the lessons of 9/11, Congress and federal departments have taken steps to improve information sharing across the federal government and in conjunction with state and local governments and law enforcement

agencies, as well, but these efforts are not without challenges. The FBI has increased its field Joint Terrorism Task Forces, bringing together personnel from all levels of government in their counterterrorism missions.[101] DHS implemented the homeland security information network to share homeland security information with states, localities, and the private sector. States and localities are creating their own information "fusion" centers, some with FBI and DHS support, to provide state and local leaders with information on threats to their communities, a topic on which we have ongoing work. And DHS has implemented a program to encourage the private sector to provide information on the vulnerabilities and security in place at critical infrastructure assets, such as nuclear and chemical facilities by guaranteeing to protect that information from public disclosure. But, the DHS Inspector General found that users of the homeland security information network were confused and frustrated with this system, in part because the system does not provide them with useful situational awareness and classified information and as a result users do not regularly use the system; how well fusion centers will be integrated into the federal information sharing efforts remains to be seen. And DHS has still not won all of the private sector's trust that the agency can adequately protect and effectively use the information that sector provides. These challenges will require longer-term actions to resolve.

These challenges also require policies, procedures, and plans that integrate these individual initiatives and establish a clear, governmentwide framework for sharing terrorism-related information. But as we reported in March 2006, the nation still has not implemented the governmentwide policies and processes that the 9/11 commission recommended and that Congress mandated.[102] Responsibility for creating these policies has shifted over time—from the White House to the Office of Management and Budget, to the Department of Homeland Security, and then to the Office of the Director of National Intelligence. Nevertheless, the Intelligence Reform and Terrorism Prevention Act required that action be taken to facilitate the sharing of terrorism information by establishing an "information sharing environment" that would combine policies, procedures, and technologies that link people, systems, and information among all appropriate federal, state, local, and tribal entities and the private sector.

---

[101]GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.: Mar. 17, 2006).

[102]See GAO-06-385.

One purpose of this information sharing environment is to represent a partnership between all levels of government, the private sector, and our foreign partners. While this environment was to be established by December 2006, program managers told us that a 3-year road map is to be released in November 2006. According to these officials, the plan will define key tasks and milestones for developing the information sharing environment, including identifying barriers and ways to resolve them, as GAO recommended. Completing the information sharing environment is a complex task that will take multiple years and long-term administration and congressional support and oversight, and will pose cultural, operational, and technical challenges that will require a collaborated response.

## Developing and Implementing a Risk-Based Framework to Balance Trade-offs between Security and Other Priorities Remains a Critical Strategic Federal Challenge

Addressing the diffuse nature of terrorist threats—and protecting the vast array of assets and infrastructure potentially vulnerable to attack—requires trade-offs that balance security needs with competing priorities for limited resources. Shortly after 9/11, new federal policies sought to acknowledge the importance of determining these trade-offs. For example, as reflected in the National Strategy for Homeland Security of 2002, the United States is to "carefully weigh the benefit of each homeland security endeavor and only allocate resources where the benefit of reducing risk is worth the amount of additional cost." The strategy recognizes that the need for homeland security is not tied solely to the current terrorist threat but to enduring vulnerability from a range of potential threats that could include weapons of mass destruction and bioterrorism. In addition, Homeland Security Presidential Directive-7, issued in December 2003, charged DHS with integrating the use of risk management into homeland security activities related to the protection of critical infrastructure. The directive called for the department to develop policies, guidelines, criteria, and metrics for this effort.

Federal officials are also well aware of the need for taking a risk-based approach to allocating scarce resources for homeland security. The Secretary of DHS testified in June 2005 on the need for managing risk by developing plans and allocating resources in a way that balances security and freedom. He noted the importance of assessing the full spectrum of threats and vulnerabilities, conducting risk assessments, setting realistic priorities, and guiding decisions about how to best organize to prevent, respond to, and recover from an attack.

In our January 2005 report on high-risk areas in the federal government,[103] we noted the importance of completing comprehensive national threat and risk assessments—and noted risk management as an emerging area. At that time, we noted that DHS was in the early stages of adopting a risk-based strategic framework for making important resource decisions involving billions of dollars annually. In part, this is because the process is difficult and complex; requires comprehensive information on risks and vulnerabilities; and employs sophisticated assessment methodologies. The process also requires careful trade-offs that balance security concerns with economic interests and other competing interests. DHS, with a fiscal year 2007 budget of about $35 billion, has begun allocating grants based on risk criteria, and has begun risk assessments at individual infrastructure facilities. But, it has not completed all of the necessary risk assessments mandated by the Homeland Security Act of 2002 to set priorities to help focus its resources where most needed. In addition, when applying risk management to critical infrastructure protection, DHS's risk management framework, which requires the support of a comprehensive, national inventory of critical infrastructure assets that DHS refers to as the National Asset Database, remains incomplete. And, according to the DHS OIG, the agency is still identifying and collecting critical infrastructure data for this tool and this database is not yet comprehensive enough to support the management and resource allocation decisionmaking needed to meet the requirements of HSPD-7.[104]

Nonetheless, agencies are making progress in using risk as a basis for decision making. We found, for example, that the Coast Guard had made the greatest progress among three DHS agencies we reviewed in conducting risk assessments—that is, evaluating individual threats, the degree of vulnerability to attack, and the consequences of a successful attack.[105] Also, we found that TSA has begun to assess risks within other transportation modes, such as rail in an effort to begin allocating scarce

---

[103]GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005); GAO, *Strategic Budgeting: Risk Management Principles Can Help DHS Allocate Resources to Highest Priorities*, GAO-05-824T (Washington, D.C: June 29, 2005).

[104]Department of Homeland Security Office of Inspector General, *Progress in Developing the National Asset Database*, OIG-06-40 (Washington, D.C.: June 10, 2006).

[105]GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91 (Washington, D.C.: Dec. 15, 2005).

GAO-07-375  Progress to Address Security After 9/11

resources toward the greatest risks and vulnerabilities.[106] Nevertheless, DHS is still faced with the formidable task of developing a more formal and disciplined approach to risk management, and answering questions such as what is an acceptable level of risk to guide homeland security strategies and investments and what criteria should be used to target federal funding for homeland security to maximize results and mitigate risks within available resource levels. Doing so will not be easy. However, as we noted in our analysis of homeland security challenges for the 21st century, defining an acceptable, achievable level of risk, within constrained budgets is imperative to addressing current and future threats.[107]

In the longer term, progress in implementing a risk-based approach will rest heavily on how well DHS coordinates homeland security risk management efforts with other federal departments, as well as state, local, and private-sector partners that oversee or operate critical infrastructure and assets. Currently, our work shows that while various risk assessment approaches are being used within DHS, they are neither consistent nor comparable—that is, there is no common basis, or framework, used to evaluate risk assessments within sectors (such as transportation) or across sectors (such as transportation, energy, and agriculture). DHS faces challenges related to establishing uniform assessment policies, approaches, guidelines, and methodologies so that a common risk framework can be developed and implemented within and across sectors. Overall, DHS has much more to do to effectively manage risk as part of its homeland security responsibilities within current and expected resource levels.

## DHS Faces Challenges in Managing Its Organizational Transformation

DHS faces significant management and organizational transformation challenges as it works to protect the nation from terrorism and simultaneously establish itself. It must continue to integrate approximately 180,000 employees from 22 originating agencies, consolidate multiple management systems and processes, and transform into a more effective organization with robust planning, management, and operations. For these reasons, in January 2005, we continued to designate the implementation and transformation of the department as high risk. DHS's Inspector

---

[106]GAO, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO-06-181T (Washington, D.C.: Oct. 20, 2005).

[107]GAO, *21st Century Challenges: Reexamining the Base of the Federal Government*, GAO-05-325SP (Washington, D.C.: February 2005).

General also reported, in December 2004, that integrating DHS's many separate components into a single effective, efficient and economical department remains one of its biggest challenges. Failure to effectively address these management challenges could have serious consequences for our national security.

This task of transforming 22 agencies—several with major management challenges—into one department with the critical, core mission of protecting the country against another terrorist attack has presented many challenges to the Department's managers and employees. While DHS has made progress, it still has much to do to establish a cohesive, efficient and effective organization. Successful transformations of large organizations, even those faced with less strenuous reorganizations and pressure for immediate results than DHS, can take from 5 to 7 years to take hold on a sustainable basis. For DHS to successfully address its daunting management challenges and transform itself into a more effective organization, we have stated that it needs to take the following actions:

- develop a department wide implementation and transformation strategy that adopts risk management and strategic management principles and establishes key milestones and performance measures;

- improve management systems including financial systems, information management, human capital, and acquisitions; and

- implement corrective actions to address programmatic and partnering challenges.

The DHS OIG, in its report on the major management challenges facing DHS, identified consolidating the department's components as a challenge, but noted that the 2005 departmental restructuring has resulted in changes to the DHS organizational structure that refocused it on risk and consequence management and further involved its partners in other federal agencies, state and local governments, and private sector organizations.[108] However, the IG concluded that much more remains to be done.

---

[108]Department of Homeland Security Office of Inspector General, *Major Management Challenges Facing the Department of Homeland Security*, OIG-06-14 (Washington, D.C.: December 2005).

**GAO-07-375 Progress to Address Security After 9/11**

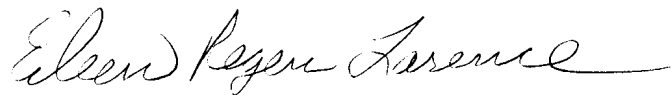| GAO Concluding Observations—Strategic Challenges | After spending billions of dollars on people, policies, procedures, and technology to improve security, we have improved preparedness compared to the time of the attacks, but much more needs to be done as terrorists change tactics and introduce new vulnerabilities. Consequently, we must remain ever vigilant. Today, we are more alert to the possibility of threats. DHS is engaged in a number of individual efforts and initiatives as it works to implement its vision of an integrated, unified department. The momentum generated by the attacks of 9/11 to create a successful homeland security function could be lost if DHS does not continue to work quickly to put in place key merger and transformation practices that would enable it to be more effective in taking a comprehensive and sustained approach to its management integration. Moreover, it remains vitally important for DHS to continue to develop and implement a risk-based framework to help target where the nation's resources should be invested to strengthen security, and determine how these investments should be directed—toward people, processes, or technology. And we must continue to improve the sharing of terrorism-related information across organizational and intergovernmental cultures and "stovepipes." Finally, Congress continues to play an important role in overseeing the nation's homeland security efforts, and has asked GAO to assist in this oversight. Our work, the work of the Inspectors General, and the work of other accountability organizations has helped identify where Congress can provide solutions and enhance our homeland security investments. |
| --- | --- |

We will send copies of this report to the Secretary of Homeland Security, the Secretary of the Department of State, and interested congressional committees. We will make copies available to others upon request. In addition, this report will be available at no charge on GAO's Web site at http://www.gao.gov.

If you have any questions about this report, please contact me at larencee@gao.gov or (202) 512-8777. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix V.

Sincerely,

Eileen Larence
Director, Homeland Security and Justice Issues

# Appendix I: Visas Issued to the September 11, 2001, Terrorist Hijackers

The 19 hijackers who participated in the September 11 terrorist attacks received a total of 23 visas at five different consular posts from April 1997 through June 2001 (see fig. 6). Fifteen of them were citizens of Saudi Arabia. They obtained their visas in their home country, at the U.S. consulate in Jeddah (11 hijackers) and the U.S. embassy in Riyadh (4 hijackers). Two others, citizens of the United Arab Emirates, also received their visas in their home country, at the U.S. embassy in Abu Dhabi and at the U.S. consulate in Dubai. The remaining 2 hijackers obtained their visas at the U.S. embassy in Berlin. They were considered third-country national applicants because they were not German citizens: one was a citizen of Egypt, the other of Lebanon. Of the 19 hijackers, 18 received visas for temporary visits for business and pleasure, and 1 received 2 student visas. These visas allowed the holders to enter the United State multiple times during the visas' validity period, subject to the approval of the immigration officer at the port of entry. Of the 23 issued visas, 4 were valid for a period of 1 year; 15 were valid for 2 years; 2 for 5 years; and 2 for 10 years.

**Figure 6: Timeline of Visas issued to Hijackers at Overseas Posts, November 1997 through June 2001**

| 1997 | 1999 | 2000 | | | | | | 2001 | |
|---|---|---|---|---|---|---|---|---|---|
| November | April | January | May | September | October | November | | April | June |

**1/18-Dubai**
Marwan Al Shehhi

**9/3-Jeddah**
Ahmed Al Ghamdi

**5/18-Berlin**
Mohamed Atta

**10/17-Riyadh**
Hamza Al Ghamdi

**11/12-Jeddah**
Ahmad Al Haznawi

**4/3-Jeddah**
Nawaf Al Hazmi

**5/25-Berlin**
Ziad Jarrah

**9/4-Jeddah**
Saeed Al Ghamdi
*(1st visa)*

**6/12-Jeddah**
Saeed Al Ghamdi
*(2nd visa)*

**11/20-Riyadh**
Majed Moqed

**4/7-Jeddah**
Khalid Al Mihdhar
*(1st visa)*

**6/13-Jeddah**
Khalid Al Mihdhar
*(2nd visa)*

**10/23-Riyadh**
Mohand Al Shehri

**11/21-Riyadh**
Satam Al Suqami

**11/2-Jeddah**
Hani Hanjour
*(1st student visa)*

**9/25-Jeddah**
Hani Hanjour
*(2nd student visa)*

**10/24-Jeddah**
Wail Al Shehri

**6/18-Jeddah**
Abdul Al Omari

**10/24-Jeddah**
Waleed Al Shehri

**6/18-Abu Dhabi**
Fayez Banihammad

**10/28-Jeddah**
Ahmed Al Nami
*(1st visa)*

**4/23-Jeddah**
Ahmed Al Nami
*(2nd visa)*

**6/20-Jeddah**
Salem Al Hazmi

Source: State Department.

# Appendix II: Map of Visa Waiver Program Countries



Japan

Brunei

Singapore

Australia

New Zealand

Norway

Iceland

Finland

Sweden

United Kingdom

Denmark

The Netherlands

Germany

Belgium

Ireland

Luxembourg

Austria

France

Slovenia

Liechtenstein

Spain

Portugal

Italy

San Marino

Monaco

Switzerland

Andorra
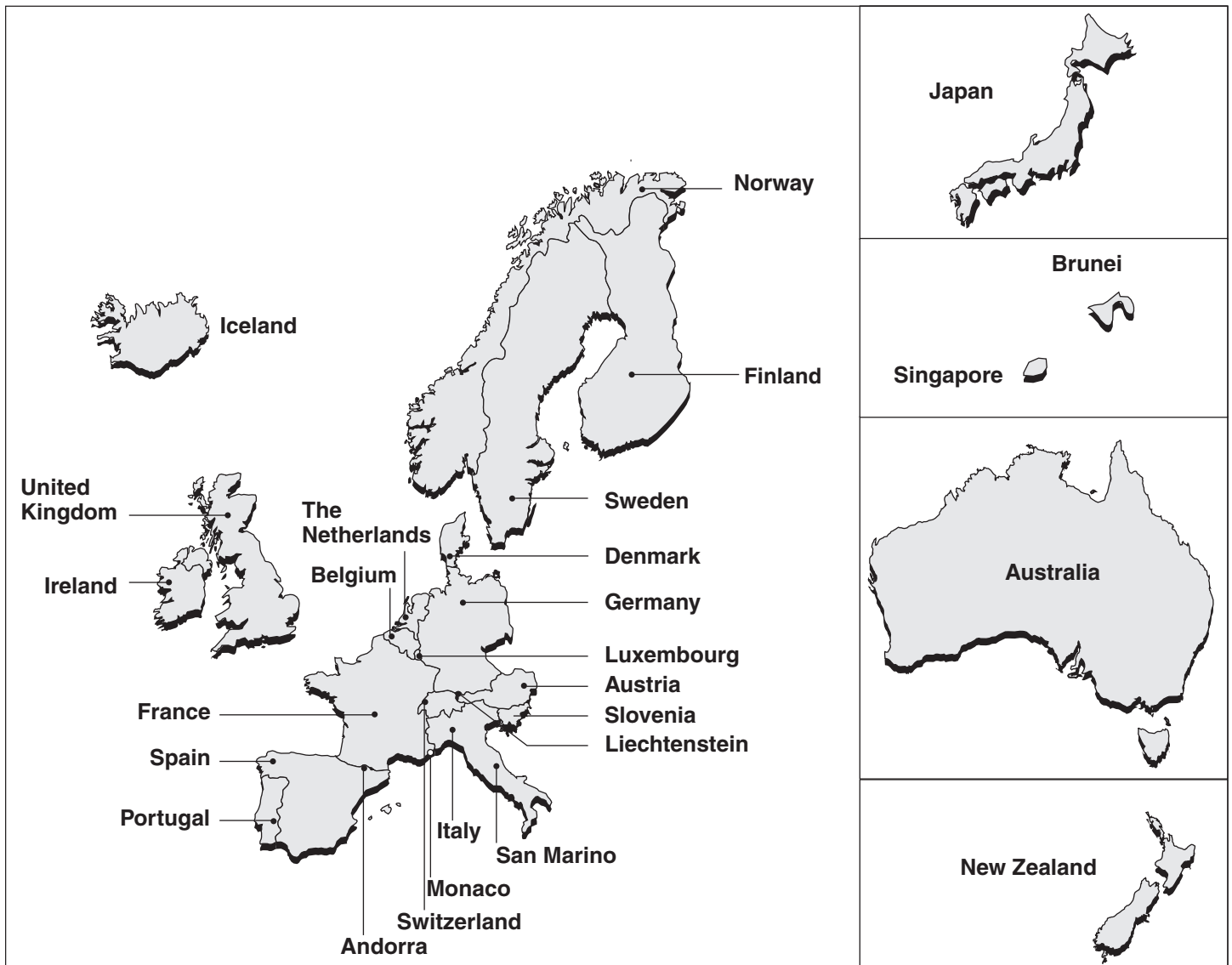
Sources: GAO; MapArt (image).

# Appendix III: Related GAO and Inspectors General Products

## Transportation Security

### Aviation Security

Passenger Prescreening and Checkpoint Screening

*Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues Remain.* GAO-07-55SU. Washington, D.C.: Nov. 20, 2006.

*Transportation Security Administration's Office of Intelligence: Responses to Post Hearing Questions on Secure Flight.* GAO-06-1051R. Washington D.C.: August 4, 2006.

*Aviation Security: Management Challenges Remain for the Transportation Security Administration's Secure Flight Program.* GAO-06-864T. Washington D.C.: June 14, 2006.

*Aviation Security: Enhancements Made in Passenger and Checked Baggage Screening, but Challenges Remain.* GAO-06-371T. Washington, D.C.: April 4, 2006.

*Aviation Security: Transportation Security Administration Has Made Progress in Managing a Federal Security Workforce and Ensuring Security at U.S. Airports, but Challenges Remain.* GAO-06-597T. Washington, D.C.: April 4, 2006.

*Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program.* GAO-06-374T. Washington, D.C.: Feb. 9, 2006.

*Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information During Secure Flight Program Testing in Initial Privacy Notes, but Has Recently Taken Steps to More Fully Inform the Public.* GAO-05-864R. Washington, D.C.: July 22, 2005.

*Aviation Security: Screener Training and Performance Measurement Strengthened, but More Work Remains.* GAO-05-457. Washington, D.C.: May 2, 2005.

*Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed.* GAO-05-356. Washington, D.C.: March 28, 2005.

*Follow-Up Audit of Passenger and Baggage Screening Procedures at Domestic Airports (Unclassified Summary).* Department of Homeland Security Office of Inspector General, OIG-05-16. Washington, D.C.: March 2005.

*Aviation Security: Measures for Testing the Effect of Using Commercial Data for the Secure Flight Program.* GAO-05-324. Washington, D.C.: Feb. 23, 2005.

*Aviation Security: Challenges Delay Implementation of Computer-Assisted Passenger Prescreening System.* GAO-04-504T. Washington, D.C.: March 17, 2004.

*Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges.* GAO-04-385. Washington, D.C.: Feb. 13, 2004.

*Aviation Security: Challenges Exist in Stabilizing and Enhancing Passenger and Baggage Screening Operations.* GAO-04-440T. Washington, D.C.: Feb. 12, 2004.

*Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining.* GAO-03-1173. Washington, D.C.: Sept. 24, 2003.

In-Flight Security

*Aviation Security: Further Study of Safety and Effectiveness and Better Management Controls Needed If Air Carriers Resume Interest in Deploying Less-than-Lethal Weapons.* GAO-06-475. Washington, D.C.: May 26, 2006.

*Aviation Security: Federal Air Marshal Service Could Benefit from Improved Planning and Controls,* GAO-06-203. Washington, D.C.: Nov. 28, 2005.

*Aviation Security: Flight and Cabin Crew Member Security Training Strengthened, but Better Planning and Internal Controls Needed.* GAO-05-781. Washington, D.C.: Sept. 6, 2005.

*Aviation Security: Federal Air Marshal Service Is Addressing Challenges of Its Expanded Mission and Workforce, but Additional Actions Needed.* GAO-04-242. Washington, D.C.: Nov. 19, 2003.

*Aviation Security: Information Concerning the Arming of Commercial Pilots.* GAO-02-822R. Washington, D.C.: June 28, 2002.

Checked Baggage Screening

*Aviation Security: TSA Oversight of Checked Baggage Screening Procedures Could Be Strengthened.* GAO-06-869. Washington, D.C.: July 28, 2006.

*Aviation Security: TSA Has Strengthened Efforts to Plan for the Optimal Deployment of Checked Baggage Screening Systems but Funding Uncertainties Remain.* GAO-06-875T. Washington, D.C.: June 29, 2006

*Aviation Security: Better Planning Needed to Optimize Deployment of Checked Baggage Screening Systems.* GAO-05-896T. Washington, D.C.: July 13, 2005.

*Aviation Security: Systematic Planning Needed to Optimize the Deployment of Checked Baggage Screening Systems.* GAO-05-365. Washington, D.C.: March 15, 2005.

Air Cargo

*Aviation Security: Federal Action Needed to Strengthen Domestic Air Cargo Security.* GAO-06-76. Washington, D.C.: Oct. 17, 2005.

*Aviation Security: Federal Action Needed to Strengthen Domestic Air Cargo Security.* GAO-05-446SU. Washington, D.C.: July 29, 2005.

*Aviation Safety: Undeclared Air Shipments of Dangerous Goods and DOT's Enforcement Approach.* GAO-03-22. Washington, D.C.: Jan. 10, 2003.

*Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System.* GAO-03-344. Washington, D.C.: Dec. 20, 2002.

Perimeter Security, Access Controls, and General Aviation

*Homeland Security: Agency Resources Address Violations of Restricted Airspace, but Management Improvements Are Needed.* GAO-05-928T. Washington, D.C.: July 21, 2005.

*General Aviation Security: Increased Federal Oversight Is Needed, but Continued Partnership with the Private Sector Is Critical to Long-Term Success.* GAO-05-144. Washington, D.C.: Nov. 10, 2004.

*Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls.* GAO-04-728. Washington, D.C.: June 4, 2004.

*Aviation Security: Challenges in Using Biometric Technologies.* GAO-04-785T. Washington, D.C.: May 19, 2004.

*Nonproliferation: Further Improvements Needed in U.S. Efforts to Counter Threats from Man-Portable Air Defense Systems.* GAO-04-519. Washington, D.C.: May 13, 2004.

*Aviation Security: Factors Could Limit the Effectiveness of the Transportation Security Administration's Efforts to Secure Aerial Advertising Operations.* GAO-04-499R. Washington, D.C.: March 5, 2004.

*The Department of Homeland Security Needs to Fully Adopt a Knowledge-based Approach to Its Counter-MANPADS Development Program.* GAO-04-341R. Washington, D.C.: Jan. 30, 2004.

## Other Aviation Security

*Transportation Security Administration: More Clarity on the Authority of Federal Security Directors Is Needed.* GAO-05-935. Washington, D.C.: Sept. 23, 2005.

*Aviation Security: Improvement Still Needed in Federal Aviation Security Efforts.* GAO-04-592T. Washington, D.C.: March 30, 2004.

*Aviation Security: Efforts to Measure Effectiveness and Strengthen Security Programs.* GAO-04-285T. Washington, D.C.: Nov. 20, 2003.

*Aviation Security: Efforts to Measure Effectiveness and Address Challenges.* GAO-04-232T. Washington, D.C.: Nov. 5, 2003.

*Aviation Security: Progress Since September 11, 2001, and the Challenges Ahead.* GAO-03-1150T. Washington, D.C.: Sept. 9, 2003.

*Airport Finance: Past Funding Levels May Not Be Sufficient to Cover Airports' Planned Capital Development.* GAO-03-497T. Washington, D.C.: Feb. 25, 2003.

*Aviation Security Costs, Transportation Security Agency.* Department of Homeland Security Office of Inspector General, CC-003-066. Washington, D.C.: Feb 5, 2003.

*Airport Finance: Using Airport Grant Funds for Security Projects Has
Affected Some Development Projects.* GAO-03-27. Washington, D.C.:
Oct. 15, 2002.

*Commercial Aviation: Financial Condition and Industry Responses
Affect Competition.* GAO-03-171T. Washington, D.C.: Oct. 2, 2002.

*Aviation Security: Transportation Security Administration Faces
Immediate and Long-Term Challenges.* GAO-02-971T. Washington, D.C.:
July 25, 2002.

*Challenges Facing TSA in Implementing the Aviation and
Transportation Security Act.* Department of Homeland Security Office of
Inspector General, CC-2002-88. Washington, D.C.: Jan. 23, 2002.

*Aviation Security: Vulnerabilities in, and Alternatives for, Preboard
Screening Security Operations.* GAO-01-1171T. Washington, D.C.:
Sept. 25, 2001.

*Actions Needed to Improve Aviation Security.* Department of Homeland
Security Office of Inspector General, CC-2001-313. Washington, D.C.: Sept.
25, 2001.

*Aviation Security: Weaknesses in Airport Security and Options for
Assigning Screening Responsibilities.* GAO-01-1165T. Washington, D.C.:
Sept. 21, 2001.

*Aviation Security: Terrorist Acts Demonstrate Urgent Need to Improve
Security at the Nation's Airports.* GAO-01-1162T. Washington, D.C.:
Sept. 20, 2001.

*Aviation Security: Terrorist Acts Illustrate Severe Weaknesses in
Aviation Security.* GAO-01-1166T. Washington, D.C.: Sept. 20, 2001.

*Aviation Security in the United States.* Department of Homeland Security
Office of Inspector General, CC-2001-308. Washington, D.C.: Sept. 20, 2001.

## Surface and Maritime Security

*Rail Transit: Additional Federal Leadership Would Enhance FTA's State
Safety Oversight Program.* GAO-06-821. Washington, D.C.: July 26, 2006.

*Maritime Security: Information-Sharing Efforts Are Improving.*
GAO-06-933T. Washington, D.C.: July 10, 2006.

*Information Technology: Customs Has Made Progress on Automated
Commercial Environment System, but It Faces Long-Standing
Management Challenges and New Risks.* GAO-06-580. Washington, D.C.:
May 31, 2006.

*Passenger Rail Security: Evaluating Foreign Security Practices and
Risk Can Help Guide Security Efforts.* GAO-06-557T. Washington, D.C.:
March 29, 2006.

*Passenger Rail Security: Enhanced Federal Leadership Needed to
Prioritize and Guide Security Efforts.* GAO-06-181T. Washington, D.C.:
Oct. 20, 2005.

*Passenger Rail Security: Enhanced Federal Leadership Needed to
Prioritize and Guide Security Efforts.* GAO-05-851. Washington, D.C.:
Sept. 9, 2005.

*Maritime Security: Enhancements Made, But Implementation and
Sustainability Remain Key Challenges.* GAO-05-448T. Washington, D.C.:
May 17, 2005.

*Maritime Security: New Structures Have Improved Information
Sharing, but Security Clearance Processing Requires Further Attention.*
GAO-05-394. Washington, D.C.: April 15, 2005.

*Information Technology: Customs Automated Commercial Environment
Program Progressing, but Need for Management Improvements
Continues.* GAO-05-267. Washington, D.C.: March 14, 2005.

*Maritime Security: Better Planning Needed to Help Ensure an Effective
Port Security Assessment Program.* GAO-04-1062. Washington, D.C.: Sept.
30, 2004.

*Mass Transit: Federal Action Could Help Transit Agencies Address
Security Challenges.* GAO-03-263. Washington, D.C.: Dec. 13, 2002.

## General Transportation Security

*Transportation Security: DHS Should Address Key Challenges Before
Implementing the Transportation Worker Identification Program.*
GAO-06-982. Washington, D.C.: September 2006.

*Transportation Security: Systematic Planning Needed to Optimize
Resources.* GAO-05-357T. Washington, D.C.: Feb. 15, 2005.

*Transportation Security R&D: TSA and DHS Are Researching and Developing Technologies, but Need to Improve R&D Management.* GAO-04-890. Washington, D.C.: Sept. 30, 2004.

*Transportation Security: Federal Action Needed to Enhance Security Efforts.* GAO-03-1154T. Washington, D.C.: Sept. 9, 2003.

*Transportation Security: Federal Action Needed to Help Address Security Challenges.* GAO-03-843. Washington, D.C.: June 30, 2003.

*Federal Aviation Administration: Reauthorization Provides Opportunities to Address Key Agency Challenges.* GAO-03-653T. Washington, D.C.: April 10, 2003.

*Transportation Security: Post-September 11th Initiatives and Long-Term Challenges.* GAO-03-616T. Washington, D.C.: April 1, 2003.

*Transportation Security Administration: Actions and Plans to Build a Results-Oriented Culture.* GAO-03-190. Washington, D.C.: Jan. 17, 2003.

# Border Security

## Visa Process and Visa Waiver Program

*Border Security: Stronger Actions Needed to Assess and Mitigate Risks of the Visa Waiver Program.* GAO-06-1090T. Washington, D.C.: Sept. 7, 2006.

*Border Security: Stronger Actions Needed to Assess and Mitigate Risks of the Visa Waiver Program.* GAO-06-854. Washington, D.C.: July 28, 2006.

*Process for Admitting Additional Countries into the Visa Waiver Program.* GAO-06-835R. Washington, D.C.: July 28, 2006.

*Border Security: More Emphasis on State's Consular Safeguards Could Mitigate Visa Malfeasance Risks.* GAO-06-115. Washington, D.C.: Oct. 6, 2005.

*Border Security: Strengthened Visa Process Would Benefit From Improvements in Staffing and Information Sharing.* GAO-05-859. Washington, D.C.: Sept. 13, 2005.

*Border Security: Actions Needed to Strengthen Management of
Department of Homeland Security's Visa Security Program.* GAO-05-801.
Washington, D.C.: July 29, 2005.

*Border Security: Reassessment of Consular Security Resource
Requirements Could Help Address Visa Delays.* GAO-06-542T.
Washington, D.C.: April 4, 2005.

*Border Security: Streamlined Visas Mantis Program Has Lowered
Burden on Foreign Science Students and Scholars, but Further
Refinements Needed.* GAO-05-198. Washington, D.C.: Feb. 18, 2005.

*Implementation of the United States Visitor and Immigrant Status
Indicator Technology Program at Land Border Ports of Entry.*
Department of Homeland Security Office of Inspector General, OIG-05-11.
Washington, D.C.: Feb. 2005.

*A Review of the Use of Stolen Passports from Visa Waiver Countries to
Enter the United States.* Department of Homeland Security Office of
Inspector General, OIG-05-07. Washington, D.C.: Dec. 2004.

*Border Security: State Department Rollout of Biometric Visas on
Schedule, but Guidance Is Lagging.* GAO-04-1001. Washington, D.C.:
Sept. 9, 2004.

*An Evaluation of DHS Activities to Implement Section 428 of the
Homeland Security Act of 2002.* Department of Homeland Security Office
of Inspector General, OIG-04-33. Washington, D.C.: August 2004.

*Border Security: Additional Actions Needed to Eliminate Weaknesses in
the Visa Revocation Process.* GAO-04-795. Washington, D.C.: July 13, 2004.

*An Evaluation of the Security Implications of the Visa Waiver Program.*
Department of Homeland Security Office of Inspector General, OIG-04-26.
Washington, D.C.: April 2004.

*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.

*Border Security: New Policies and Increased Interagency Coordination
Needed to Improve Visa Process.* GAO-03-1013T. Washington, D.C.: July
15, 2003.

*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.

*Review of Nonimmigrant Visa Policy and Procedures*, memorandum report. Department of State Office of Inspector General, ISP-I-03-26. Washington, D.C.: Dec. 2002.

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

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

## US-VISIT and Other Border Security Issues

*Border Security: US-VISIT Faces Strategic, Technological, and Operational Challenges at Land Ports of Entry.* GAO-07-248. Washington, D.C.: Dec. 06, 2006.

*Border Security: Continued Weaknesses in Screening Entrants into the United States.* GAO-06-976T. Washington, D.C.: August 2, 2006.

*Information Technology: Immigration and Customs Enforcement Is Beginning to Address Infrastructure Modernization Program Weaknesses but Key Improvements Still Needed.* GAO-06-823. Washington, D.C.: July 27, 2006.

*Homeland Security: Contract Management and Oversight for Visitor and Immigrant Status Program Need to Be Strengthened.* GAO-06-404. Washington, D.C.: June 9, 2006.

*Observations on Efforts to Implement Western Hemisphere Travel Initiative on the U.S. Border with Canada.* GAO-06-741. Washington, D.C.: May 25, 2006.

*Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System.* GAO-06-591T. Washington, D.C.: March 30, 2006.

*Border Security: Investigators Successfully Transported Radioactive Sources Across Our Nation's Borders at Selected Locations.* GAO-06-545R. Washington, D.C.: March 28, 2006.

*Combating Nuclear Smuggling: DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports-of-Entry, but Concerns Remain.* GAO-06-389. Washington, D.C.: March 22, 2006.

*Combating Nuclear Smuggling: Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries.* GAO-06-311. Washington, D.C.: March 14, 2006.

*Homeland Security: Visitor and Immigrant Status Program Operating, but Management Improvements Are Still Needed.* GAO-06-318T. Washington, D.C.: Jan. 25, 2006.

*Cargo Security: Partnership Program Grants Importers Reduced Scrutiny With Limited Assurance of Improved Security.* GAO-05-404. Washington, D.C.: March 11, 2005.

*US-VISIT System Security Management Needs Strengthening (Redacted).* Department of Homeland Security Office of Inspector General. OIG-06-16. Washington, D.C.: Dec. 2005.

*Information Technology: Management Improvements Needed on Immigration and Customs Enforcement's Infrastructure Modernization Program.* GAO-05-805. Washington, D.C.: Sept. 7, 2005.

*Review of the Immigration and Customs Enforcement Compliance Enforcement Unit.* Department of Homeland Security Office of Inspector General, OIG-05-50. Washington, D.C.: Sept. 2005.

*Border Security: Opportunities to Increase Coordination of Air and Marine Assets.* GAO-05-543. Washington, D.C.: August 12, 2005.

*Homeland Security: Key Cargo Security Programs Can Be Improved.* GAO-05-466T. Washington, D.C.: May 26, 2005.

*Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts.* GAO-05-557. Washington, D.C.: April 26, 2005.

*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.

*Implementation of the United States Visitor and Immigrant Status
Indicator Technology Program at Land Border Ports of Entry.*
Department of Homeland Security Office of Inspector General, OIG-05-11.
Washington, D.C.: Feb. 2005.

*Homeland Security: Management Challenges Remain in Transforming
Immigration Programs.* GAO-05-81. Washington, D.C.: Oct. 14, 2004.

*Immigration Enforcement: DHS Has Incorporated Immigration
Enforcement Objectives and Is Addressing Future Planning
Requirements.* GAO-05-66. Washington, D.C.: Oct. 8, 2004.

*Overstay Tracking: A Key Component of Homeland Security and a
Layered Defense.* GAO-04-82. Washington, D.C.: May 21, 2004.

*Homeland Security: First Phase of Visitor and Immigration Status
Program Operating, but Improvements Needed.* GAO-04-586. Washington,
D.C.: May 11, 2004.

*Security: Counterfeit Identification Raises Homeland Security
Concerns.* GAO-04-133T. Washington, D.C.: Oct. 1, 2003.

*Homeland Security: Risks Facing Key Border and Transportation
Security Program Needs to Be Addressed.* GAO-03-1083. Washington, D.C.:
Sept. 19, 2003.

*Security: Counterfeit Identification and Identification Fraud Raise
Security Concerns.* GAO-03-1147T. Washington, D.C.: Sept. 9, 2003.

*Land Border Ports of Entry: Vulnerabilities and Inefficiencies in the
Inspections Process.* GAO-03-1084R. Washington, D.C.: Aug. 18, 2003.

*Counterfeit Documents Used to Enter the Country from Certain Western
Hemisphere Countries Not Detected.* GAO-03-713T. Washington, D.C.: May
13, 2003.

*Weaknesses in Screening Entrants into the United States.* GAO-03-438T.
Washington, D.C.: Jan. 30, 2003.

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

# Watch List and Information Sharing

*Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics.* GAO-07-39. Washington, D.C.: Oct. 2006.

*Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public.* GAO-06-1031. Washington, D.C.: Sept. 29, 2006.

*Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity.* GAO-06-1087T. Washington, D.C.: Sept. 13, 2006.

*Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information.* GAO-06-383. Washington, D.C.: April 17, 2006.

*Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information.* GAO-06-385. Washington, D.C.: March 17, 2006.

*Review of the Terrorist Screening Center.* Department of Homeland Security Office of Inspector General, Audit Report 05-27. Washington, D.C.: June 2005.

*DHS Challenges in Consolidating Terrorist Watch List Information.* Department of Homeland Security Office of Inspector General, OIG-04-31. Washington, D.C.: Aug. 2004.

*Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors.* GAO-04-780. Washington, D.C.: July 9, 2004.

*Homeland Security: Communication Protocols and Risk Communication Principles Can Assist in Refining the Advisory System.* GAO-04-682. Washington, D.C.: June 25, 2004

*Homeland Security: Efforts to Improve Information Sharing Need to be Strengthened.* GAO-03-760. Washington, D.C.: August 27, 2003

*Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing.* GAO-03-322. Washington, D.C.: April 15, 2003.

# Homeland Security, Risk Management, and High Risk List

*GAO's High Risk Program.* GAO-06-497T. Washington, D.C.: March 15, 2006.

*Progress in Developing the National Asset Database.* Department of Homeland Security Office of Inspector General, OIG-06-40. Washington, D.C.: June 10, 2006.

*Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure.* GAO-06-91. Washington, D.C.: Dec. 15, 2005.

*Major Management Challenges Facing the Department of Homeland Security.* Department of Homeland Security Office of Inspector General, OIG-06-14. Washington, D.C.: Dec. 2005.

*Department of Homeland Security: Strategic Management of Training Important for Successful Transformation.* GAO-05-888. Washington, D.C: Sept. 23, 2005.

*Strategic Budgeting: Risk Management Principles Can Help DHS Allocate Resources to Highest Priorities.* GAO-05-824T. Washington, D.C.: June 29, 2005.

*Homeland Security: Overview of Department of Homeland Security Management Challenges.* GAO-05-573T. Washington, D.C.: April 20, 2005.

*Department of Homeland Security: A Comprehensive and Sustained Approach Needed to Achieve Management Integration.* GAO-05-139. Washington, D.C.: March 16, 2005.

*21st Century Challenges: Reexamining the Base of the Federal Government.* GAO-05-325SP. Washington, D.C.: Feb. 2005.

*High-Risk Series: An Update.* GAO-05-207. Washington, D.C.: Jan. 2005.

*Homeland Security: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security.* GAO-05-33. Washington, D.C.: Jan. 14, 2005.

*9/11 Commission Report: Reorganization, Transformation, and Information Sharing.* GAO-04-1033T. Washington, D.C.: Aug. 3, 2004.

*Status of Key Recommendations GAO Has Made to DHS and Its Legacy Agencies.* GAO-04-865R. Washington, D.C.: July 2, 2004.

*Homeland Security: Selected Recommendations from Congressionally Chartered Commissions and GAO.* GAO-04-591. Washington, D.C.: March 31, 2004.

*Major Management Challenges and Program Risks: Department of State.* GAO-03-107. Washington, D.C.: Jan. 1, 2003.

*Homeland Security: A Framework for Addressing the Nation's Efforts.* GAO-01-1158T. Washington, D.C.: Sept. 21, 2001.

# Appendix IV: Comments from the Department of Homeland Security

**Homeland Security**

December 1, 2006

Ms. Eileen Larence
Director
Homeland Security and Justice Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Larence:

      RE: Draft Report GAO-07-110SU, Homeland Security: Progress Has Been Made to Address the Vulnerabilities Exposed by 9/11, but Continued Federal Action Is Needed to Further Mitigate Security Risks (GAO Job Code 440458)

The Department of Homeland Security (DHS) appreciates the opportunity to review and comment on the draft report referenced above. The Government Accountability Office (GAO) makes no new recommendations since prior recommendations on aviation security, the Visa Waiver Program, US-VISIT and other DHS related activities generally are in the process of being implemented.

We appreciate the recognition of actions taken by the Department to address vulnerabilities exposed by the terrorists' attacks of September 11, 2001. The GAO also recognizes Departmental efforts to strengthen or otherwise improve systems, equipment and oversight not directly associated with the attacks that are designed to enhance security. We realize that challenges remain and are moving forward to address them.

While the draft report is generally accurate, several statements are not currently correct or otherwise require clarification. GAO comments that the Federal government must address strategic challenges of sharing terrorism related information, managing risk, and structuring DHS to meet its mission. Specifically, GAO asserts that DHS has not completed all of the necessary risk assessments mandated by the Homeland Security Act (HLSA) of 2002 to set priorities to help focus resources where most needed. While the Department has not completed comprehensive vulnerability assessments for every asset in every sector, it has made considerable progress by both working on cross-sector vulnerability assessment methodologies and providing tools to public and private sector partners to help identify and mitigate those vulnerabilities. Furthermore, although the HLSA states that DHS is to carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States it does not provide the number of assessments to be performed, sectors to be targeted, or which of the designated seventeen sectors should have priority attention. Therefore, GAO's assertion that "all" necessary risk assessments outlined in the legislation have not been completed by the Department is not specific enough to address without more information.
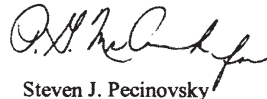
www.dhs.gov

2

GAO also asserts that DHS's risk management framework, which requires the support of a comprehensive, national inventory of critical infrastructure assets known as the National Asset Database (NADB), remains incomplete. GAO references a June 2005 Office of Inspector General report that mentions that DHS is still identifying and collecting critical infrastructure data and that this database is not yet comprehensive enough to support the management and resource allocation decision making needed to meet the requirements of HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*. We take issue with statements critical of the National Asset Database comprehensiveness and its role in supporting decision making associated with HSPD-7 requirements.

The NADB is a continually evolving and comprehensive catalog of the assets that comprise the Nation's infrastructure that contains descriptive information regarding approximately 77,000 of those assets. Since DHS uses the NADB as a "universe" from which various lists of assets can be produced, it must be viewed as an evolving resource that will change over time, reflecting the ever-changing threat environment and national protective posture. As DHS continues to query states for new assets, strengthens information gathering relationships with public and private partners, and performs database updates and upgrades over time, the NADB will fluctuate in content and breadth. The NADB catalogues infrastructure information regarding assets/systems across all 17 infrastructure sectors. It serves as a tool that supports a wide-ranging robust risk analysis process that ties together asset information, analyses concerning consequences of loss/attack, and vulnerability of an asset, system or network to the threat to those assets, systems, or networks. DHS remains committed to implementing effective risk management practices.

Technical comments are being provided under separate cover.

Sincerely,

Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison Office

MMcP

# Appendix V: GAO Contacts and Staff Acknowledgements

| | |
|---|---|
| **GAO Contacts** | Eileen Larence, Director, Homeland Security and Justice Issues, (202) 512-9286 |
| **Staff Acknowledgements** | In addition to the individual named above, key contributors to the report include Katie Bernet, Amy Bernstein, Cathleen Berrick, John Brummet, Sally Gilley, David Hooper, Kirk Kiester, Sarah Lynch, Octavia Parks, Susan Quinlan, Brian Sklar, Richard Stana, and Maria Strudwick. |