United States Government Accountability Office

GAO

Testimony

Before the Committee on Commerce, Science, and Transportation, United States Senate

For Release on Delivery
Expected at 10:00 a.m. EST
Tuesday, February 15, 2005

TRANSPORTATION SECURITY

Systematic Planning Needed to Optimize Resources

Statement of Cathleen A. Berrick, Director
Homeland Security and Justice

February 15, 2005

TRANSPORTATION SECURITY

Systematic Planning Needed to Optimize Resources

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-357T, a testimony before the Committee on Commerce, Science, and Transportation, United States Senate

Why GAO Did This Study

Critical transportation systems crisscross the nation and extend beyond our borders to move millions of passengers and tons of freight each day, making them both attractive targets to terrorists and difficult to secure. Securing these systems is further complicated by the need to balance security with the expeditious flow of people and goods through these systems. The Transportation Security Administration (TSA) faces the daunting challenge of determining how to allocate its finite resources to manage risks while addressing threats and enhancing security across all transportation modes. To assist the Congress and TSA in focusing resources on the areas of greatest need, we were asked to describe Department of Homeland Security (DHS) and TSA efforts in managing risks and allocating resources across aviation and surface transportation modes, and in integrating screening, credentialing, and research and development (R&D) efforts to achieve efficiencies.

What GAO Recommends

In prior reports, GAO has made numerous recommendations designed to strengthen transportation security. GAO also has several ongoing reviews related to the issues addressed in this testimony, and will issue separate reports related to these areas at later dates, with additional recommendations as appropriate.

www.gao.gov/cgi-bin/getrpt?GAO-05-357T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Cathleen A. Berrick at (202) 512-3404 or berrickc@gao.gov.

What GAO Found

TSA has undertaken numerous initiatives to strengthen transportation security, particularly in aviation, and its efforts should be commended. For example, since September 11, 2001, TSA has installed explosive detection systems at most of the nation's commercial airports to provide the capability to screen all checked baggage for explosives; expanded screener training and developed performance measures and indicators for the screening systems; and evaluated the security of airport perimeters and access controls and provided funding for security equipment. While these efforts are commendable, we found that TSA has not consistently implemented a risk management approach or conducted the systematic analysis needed to inform its decision-making processes and to prioritize security improvements. Our work has shown that a risk management approach can help inform decision makers in allocating finite resources to the areas of greatest need. For example, we found that since initially deploying equipment to screen checked baggage for explosive at airports in response to congressional mandates, TSA has not conducted the systematic planning needed to optimize the deployment and integration of this equipment. Limited analysis of nine airports showed that the integration of this equipment in-line with airport baggage conveyor systems—rather than continuing to maintain the equipment in a stand-alone mode—could result in significant savings for the federal government. We also found that TSA's efforts to implement a comprehensive risk management approach for its air cargo and rail security programs are ongoing.

The President's fiscal year 2006 budget request proposes two key DHS organizational changes designed to leverage resources and increase the efficiency and effectiveness of various screening, credentialing, and R&D programs. While we applaud DHS's efforts, it will be important for DHS to address several program challenges as the integration moves forward because restructuring alone will not resolve all existing challenges or ensure the successful integration and achievement of DHS's goals. These challenges including developing regulations identifying eligibility requirements for the Transportation Workers Identification Credential, establishing goals with measurable objectives in research and development strategic plans, and using risk assessments to select and prioritize research and development efforts.

Screening Passengers and Cargo are Aviation Security Concerns.

Source: FAA.

Source: Cargo King, Ltd.

Mr. Chairman and Members of the Committee:

I appreciate the opportunity to participate in today's hearing to discuss the security of our nation's transportation system and the numerous initiatives under way and planned intended to strengthen security. Following the terrorist attacks of September 11, 2001, much attention was focused on securing our commercial aviation system. Since that time, emphasis on other modes of transportation has grown as vulnerabilities are identified and highlighted, such as attempts to introduce weapons of mass destruction into the United States through ports, or to launch chemical attacks on mass transit systems. Critical transportation systems crisscross the nation and extend beyond our borders to move millions of passengers and tons of freight each day, making them both attractive targets and difficult to secure. Securing these systems is further complicated by their nature and scope, the number of stakeholders involved, and the need to balance security with the expeditious flow of people and goods through these systems. The Department of Homeland Security (DHS) and the Transportation Security Administration (TSA) face the daunting challenge of determining how to allocate their finite resources to manage risks while addressing threats and enhancing security across all transportation modes.

My testimony today describes DHS and TSA efforts in managing risks and allocating resources across aviation and surface transportation modes, and in integrating screening, credentialing, and research and development (R&D) efforts to achieve efficiencies. My comments are based on issued GAO reports and testimonies addressing the security of U.S. aviation and surface transportation systems, and our review of the President's budget request for fiscal year 2006. Appendix I contains a list of related GAO products released since September 11, 2001.

Summary

DHS and TSA have undertaken numerous initiatives to strengthen transportation security, particularly in aviation, and their efforts should be commended. Since September 11th, for example, in addition to hiring and deploying a workforce of over 40,000 airport passenger and baggage screeners, TSA has:

- Installed equipment at most of the nation's more than 400 commercial airports to provide the capability to screen all checked baggage using explosive detection systems, as mandated by Congress.
- Taken numerous steps to expand training available to the screener workforce and to develop performance measures to assess screener performance.

- Outlined a threat-based, risk-management approach for securing the air cargo transportation system.

- Taken actions to evaluate and enhance the security of airport perimeters and the controls that limit access into secured airport areas.

- Partnered with federal agencies and state governments and the general aviation industry in securing general aviation operations.

- Implemented a Screening Partnership Program through which commercial airports can apply to TSA to use private rather than federal passenger and baggage screeners.

- Issued security regulations for passenger rail assets, and begun to conduct criticality assessments of stations, tunnels, and bridges.

DHS has also proposed, in its fiscal year 2006 budget request, two key changes in its organizational structure that are designed to achieve synergy and avoid duplication of effort. These changes include creating an Office of Screening Coordination and Operations within the Border and Transportation Security Directorate that would combine several ongoing, terrorist-related screening initiatives, and consolidating its R&D efforts—currently spread across four DHS component agencies including TSA—inside its Science and Technology Directorate.

While these are commendable efforts, we also found that TSA had not always implemented a risk management approach, or conducted the systematic analysis needed, to inform its decision-making processes and to prioritize its security improvements. While we recognize that fully integrating a risk management approach is challenging for any organization, our work has shown that such an approach can help inform decision makers in allocating finite resources to the areas of greatest need. For example, we found that since the initial deployment of equipment to screen checked baggage for explosives at commercial airports in response to congressional mandates, TSA has not conducted the systematic planning needed to optimize the deployment and integration of this equipment. Limited analysis has shown that the integration of this equipment in-line with airport baggage conveyor systems—rather than maintaining the systems in a stand-alone mode—could result in significant savings for the federal government for the nine airports assessed. We also found that TSA must take a number of actions before a comprehensive risk management approach can be applied to securing air cargo. These actions include establishing complete databases of known shippers,

addressing the potential ease with which shippers may become "known," and identifying and testing security technologies in order to develop and implement a system to screen 100 percent of high risk cargo. We also found that a risk-based approach is being adopted for rail security.

In addition, while we applaud DHS's efforts to achieve efficiencies through leveraging resources and technology and improving internal coordination through proposed organizational changes, it will be important for DHS to address several challenges that have been identified with respect to these programs as the integration moves forward. Restructuring alone will not resolve all existing challenges or ensure the successful integration and achievement of DHS's goals. The challenges we identified include developing regulations identifying eligibility requirements for the Transportation Workers Identification Credential, and instituting a comprehensive plan for managing the project. DHS will also need to include goals with measurable objectives in its R&D strategic plans, prepare and use risk assessments to select and prioritize R&D projects, and coordinate with R&D stakeholders.

Background

The nation's transportation system is a vast, interconnected network of diverse modes. Key modes of transportation include aviation; highways; motor carrier (trucking); motor coach (intercity bus); maritime; pipeline; rail (passenger and freight); and transit (buses, subways, ferry boats, and light rail). The nation's transportation systems are inherently open environments, designed to move people and commerce quickly to their destinations. For example, the nation's transportation system moves over 30 million tons of freight and provides approximately 1.1 billion passenger trips each day. The diversity and size of the transportation system make it vital to our economy and national security.

TSA is responsible for the security of all modes of transportation, as outlined in the Aviation and Transportation Security Act (ATSA) (Pub. L. No. 107-71). Following the passage of ATSA, TSA began addressing two major challenges—procuring and installing explosives detection systems (EDS) and explosive trace detection (ETD) systems to

screen checked baggage for explosives,[1] and hiring and deploying federal screeners to screen passengers and their baggage at commercial airports nationwide. TSA is also tasked with managing security risks to surface transportation systems. These systems include 9 billion passenger trips per year on the nation's mass transit systems, over 161,000 miles of interstate and national highways and their integrated bridges and tunnels, and nearly 800,000 shipments of hazardous materials.

Risk Management Approach

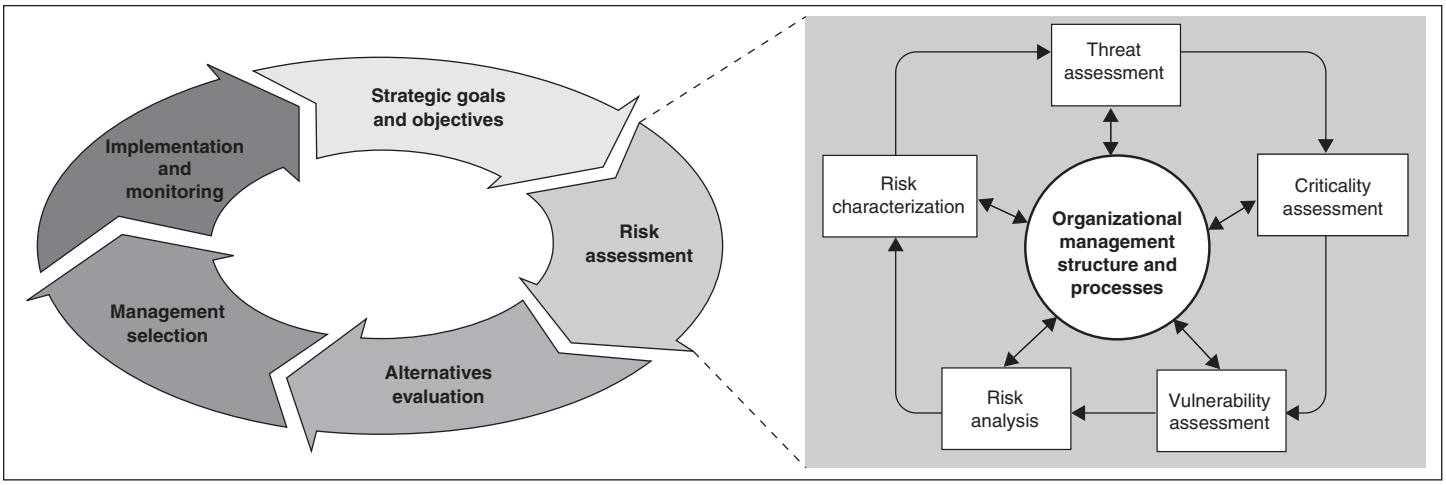
Given the vast transportation network, quick and easy access for passengers and cargo must be maintained while identifying the best possible strategies for security. The President's fiscal year 2006 budget request recognizes the need for TSA to identify, prioritize, and manage risks, and mitigate the impact of potential incidents, to help ensure that the best strategies are pursued. Consistent with this goal, GAO has advocated the need to implement—at TSA and throughout the federal government—a risk management approach for prioritizing efforts and focusing resources. A risk management approach entails a continuous process of managing risk through a series of actions, including setting strategic goals and objectives, assessing risk, evaluating alternatives, selecting initiatives to undertake, and implementing and monitoring those initiatives.

Assessing risk, a critical component of a risk management approach, involves three key elements—threats, vulnerabilities, and criticality—that provide input into the decision-making process. A threat assessment identifies and evaluates potential threats on the basis of factors such as capabilities, intentions, and past activities. A vulnerability assessment identifies weaknesses that may be exploited by identified threats and suggests options to address those weaknesses. A criticality assessment evaluates and prioritizes assets and functions in terms of specific criteria, such as their importance to public safety and the economy, as a basis for identifying which structures or processes are relatively more important to protect from attack. Information from these three assessments can lead to a risk characterization, such as high, medium, or low, and provides input

[1]EDS operates in an automated mode and use probing radiation to examine objects inside baggage and identify the characteristic signatures of threat explosives. ETD works by detecting vapors and residues of explosives. ETD requires human operators to collect samples by rubbing bags with swabs, which are chemically analyzed to identify any traces of explosive materials. References to "explosive detection systems" include both EDS and ETD systems.

for prioritizing security initiatives.[2] Figure 1 depicts a risk management cycle.

Figure 1: Risk Management Cycle



Source: GAO.

President's Budget Request for Fiscal Year 2006

In addressing security needs and challenges for all transportation modes, the President's fiscal year 2006 budget request categorizes TSA activities into three main areas: (1) Aviation Security, (2) Surface Transportation Security, and (3) Transportation Security Support.[3] Each of these areas is summarized in detail below and the total funds requested are presented in in table 1 that follows the summary.

Aviation security includes two distinct decision units: screening workforce and equipment, and aviation direction and enforcement. Screening workforce and equipment includes funding to support passenger and baggage screener activities such as screener salaries and training, and the

[2]GAO, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Washington, D.C.: October 31, 2001; and *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments*, GAO/NSIAD-98-74 (Washington, D. C.: April 9, 1998).

[3]U.S. Department of Homeland Security, Performance Budget Overview Fiscal Year 2006, Congressional Budget Justification (Washington, D.C.: February 2005); and Homeland Security Budget-in-Brief, Fiscal Year 2006 (Washington, D.C.: February 2005).

purchase and installation of screening equipment. Aviation direction and enforcement includes regulation compliance for air cargo, airports, and airlines through inspections and other efforts, and airport technology activities and administrative support. The budget requests about $5 billion for the aviation security appropriation for fiscal year 2006. These funds will support the current federalized and privatized screener workforce, provide training and other support for both passenger and baggage screening, and continue other aviation security regulation and enforcement activities. Increases were requested for, among other things, the screener workforce, checkpoint explosive detection technology, and high-speed information technology connectivity. The budget request further identified the mandatory $250 million appropriation of the Aviation Security Capital Fund to assist in the purchase, installation, and/or integration of EDS and ETD systems. At these levels, TSA expects to maintain current security and wait time performance at over 430 commercial airports.

Surface transportation security includes resources for TSA's security operations in all non-aviation modes of transportation. Such operations include developing standards and regulations to protect the transportation infrastructure; conducting inspections to monitor and enforce compliance with standards and regulations; designing and implementing vulnerability assessment models for all surface transportation modes; and facilitating information sharing with transportation stakeholders. The budget requests $32 million for surface transportation security in fiscal year 2006. These funds will be used to maintain TSA's various surface transportation security initiatives, including surface transportation inspectors added during fiscal year 2005.

Transportation security support includes funding for the operational needs of TSA's airport and field personnel and infrastructure. This area also supports TSA headquarters and the Transportation Security Intelligence Service. Although R&D funds are also included in this appropriation, the President's fiscal year 2006 budget request proposes that these funds be transferred to the DHS Science and Technology Directorate. The budget requests $545 million for transportation security support for fiscal year 2006. These funds will be used to help ensure that TSA screeners and other operational employees have sufficient intelligence information, information technology, management direction, administrative services, and other key support to accomplish the agency's mission.

Table 1: President's Fiscal Year 2006 Budget Request for TSA

	FY 2004 enacted[a]	FY 2005 enacted	FY 2006 pres. budget	FY 2006 +/- FY 2005
(dollars in thousands)				
Aviation Security[c]	$3,724,114	$4,578,523	$4,984,784	$406,261
Surface Transportation Security[c, d]	261,449	115,000	32,000	-83,000
Transportation Security Support[b, d]	592,480	711,852	545,008	-166,844
Total	**$4,578,043**	**$5,405,375**	**$5,561,792**	**$156,417**

Source: DHS.

[a]Fiscal year 2004 shows a .59 percent across-the-board enacted rescission of $13.657 million pursuant to P.L. 108-199. Fee-funded activities were exempt from rescission. Rescission was applied using Office of Management Budget discretionary fee estimates of $2,276.947 million.

[b]Fiscal year 2005 reflects transfer of $173 million in grants to Office of State and Local Government Coordination and Preparedness.

[c]Fiscal year 2006 reflects proposed transfer of Secure Flight ($34.9 million), Crew Vetting ($10 million), Credentialing Startup ($10 million), Transportation Worker Identification Credential ($50 million), Registered Traveler ($15 million), HAZMAT ($17 million), and Alien Flight School ($5 million) to the proposed new Office of Screening Coordination and Operations which is within the DHS Border and Transportation Security Directorate.

[d]Fiscal year 2006 reflects proposed research and development consolidation transferring 60 full-time equivalents and $109.040 million to the DHS Science and Technology Directorate.

TSA Has Taken Steps to Strengthen Aviation and Surface Transportation Security, but Better Planning Is Needed

TSA has taken numerous steps to strengthen aviation and surface transportation security and should be commended for its efforts. However, better planning is needed to help ensure that these initiatives are focused on the areas of greatest need to assist TSA in achieving efficiencies and enhancing security. For example, since September 11, for example, TSA has (1) installed EDS and ETD systems at most of the nation's commercial airports to provide the capability to screen all checked baggage using explosive detection systems, (2) expanded screener training and developed performance measures and indicators for the screening systems, (3) developed an air cargo strategic plan, and (4) evaluated the security of airport perimeters and access controls and provided funds for security equipment. Despite these efforts, however, we have consistently found—because of circumstances beyond TSA's control and a lack of planning—that TSA has not conducted the systematic analysis needed to inform its decision-making processes and to prioritize security enhancements. For example, we found that TSA has not always conducted needed assessments of threats, vulnerabilities, and criticality in allocating its resources, and has not fully assessed alternatives that could be pursued to achieve efficiencies and potentially enhance security. Such planning could guide TSA in moving forward in its allocation of transportation

security funding and assist it in making wise investment decisions while enhancing the security of all transportation modes.

Systematic Planning Needed to Optimize the Deployment of Checked Baggage Screening Systems

In February 2005, we reported that TSA had installed EDS and ETD systems at most of the nation's more than 400 commercial airports to provide the capability to screen all checked baggage using explosive detection systems, as mandated by Congress.[4] Despite these efforts, however, we found that in moving forward, TSA had not conducted the systematic planning needed to optimize the deployment of these systems—in particular determining at which airports EDS machines should be integrated in-line with airport baggage conveyor systems to achieve efficiencies. Such planning is important for TSA to be able to ensure that it is efficiently allocating its limited resources to maximize the effectiveness of its checked baggage screening operations and is achieving desired results.

From its creation in November 2001 through September 2004, TSA obligated[5] about $2.5 billion (93 percent) of the approximately $2.7 billion it had budgeted for fiscal years 2002 through 2004 for procuring and installing explosive detection equipment—predominantly to screen checked baggage for explosives—and making associated airport modifications to accommodate the equipment. Specifically, TSA procured and placed about 1,200 EDS machines and about 6,000 ETD machines at over 400 airports, and modified airports for the installation of this equipment. Given the congressional mandate to screen all checked baggage using explosive detection systems by December 31, 2002, later extended to December 31, 2003, TSA worked with a contractor to quickly deploy EDS and ETD equipment to the nation's airports. This response resulted in TSA placing stand-alone ETD and the minivan-sized EDS machines—usually in airport lobbies—that were not integrated in-line with airport baggage conveyor systems. Some of these interim lobby solutions resulted in operational inefficiencies, including requiring a greater number of screeners, as compared with using EDS machines in-

[4]See GAO, *Aviation Security: Systematic Planning Needed to Optimize the Deployment of Checked Baggage Screening Systems*, GAO-05-302SU (Washington, D.C.: February 4, 2005).

[5]Obligations are amounts of orders placed or contracts awarded during a given period that will require payment during the same or a future period. An administrative commitment is an administrative reservation of funds in anticipation of their obligation.

line with baggage conveyor systems. Also, screening solely with ETD machines is more labor intensive and less efficient than screening using the EDS process. TSA officials stated that they used EDS machines in a stand-alone mode and ETD machines as an interim solution in order to meet the congressional deadline for screening all checked baggage for explosives. Officials further stated that they employed these interim solutions because of the significant costs required to install in-line systems and the need to reconfigure many airports' baggage conveyor systems to accommodate the equipment. While in-line EDS baggage screening systems have a number of potential benefits, including streamlining airport and TSA operations and reducing screenings costs, these systems are capital-intensive because they often require significant airport modifications, including terminal reconfigurations, new conveyor belt systems, and electrical upgrades.

Since the initial deployment of EDS and ETD equipment, TSA has not conducted a systematic analysis of cost savings and other benefits that could be achieved from the installation of in-line baggage screening systems. However, TSA has estimated—through its limited retrospective analysis for the nine airports that received letter of intent (LOI) funding agreements[6]—that in-line baggage screening systems at these airports could save the federal government $1.3 billion over 7 years compared with stand-alone EDS systems.[7] TSA further estimated that it could recover its initial investment in the in-line systems at these airports in a little over 1 year. One factor that significantly affected estimated savings was the number of screeners required to conduct screening when using in-line baggage screening systems. According to TSA's analysis, in-line EDS systems would reduce by 78 percent the number of TSA baggage screeners and supervisors required to screen checked baggage at these nine airports, from 6,645 to 1,477. This analysis indicates the potential for cost savings through the installation of in-line EDS systems at other airports and provides insights about other key factors likely to influence potential savings. These factors include how much an airport's facilities would have to be modified to accommodate the in-line configuration; TSA's costs to buy, install, and network the EDS machines; and subsequent maintenance costs.

[6]In 2003, Congress authorized TSA to issue LOIs—a cost-sharing mechanism between TSA and the airports—to support funding the installation of in-line EDS baggage screening systems.

[7]This refers to the net present value saved over 7 years if received up front.

TSA and airport operators are relying on LOIs as their principal method for funding the modification of airport facilities to incorporate in-line baggage screening systems. The fiscal year 2003 Consolidated Appropriations Resolution approved the use of LOIs as a vehicle to leverage federal government and industry funding to support facility modification costs for installing in-line EDS baggage screening systems. When an LOI is established to provide multiyear funding for a project, the airport operator is responsible for providing—up front—the total funding needed to complete the project. Work proceeds with the understanding that TSA will, if sufficient funding is appropriated, reimburse the airport operator for a percentage of the facility modification costs, with the airport funding the remainder of the costs. The LOI does not constitute a binding commitment for federal funds.

Although airport officials we interviewed stated that they will require federal funding to install in-line systems—and TSA officials stated that additional airports would benefit from in-line systems to achieve efficiencies and for other reasons—TSA officials stated that they do not have sufficient resources in their budget to fund additional LOIs beyond the eight LOIs that have already been issued as of January 2005. These eight LOIs will support the installation of in-line baggage screening systems at nine airports for a total cost to the federal government of $957.1 million over 4 years. The Vision 100—Century of Aviation Reauthorization Act—among other things, provided for the creation of the Aviation Security Capital Fund to help pay for placing EDS machines in line with airport baggage handling systems. The President's fiscal year 2006 budget request for TSA provides approximately $240.5 million for the continued funding of the eight existing LOIs and provides no funds for new LOI agreements for in-line system integration activities.

We reported that with the objective of initially fielding EDS and ETD equipment largely accomplished, TSA needs to shift its focus from equipping airports with interim screening solutions to systematically planning for the more optimal deployment of checked baggage screening systems. Part of such planning should include analyzing which airports should receive federal support for in-line baggage screening systems based on cost savings and other benefits that could be achieved from more effective and efficient baggage screening operations. Also, for airports where in-line systems may not be economically justified, a cost-effectiveness analysis could be used to determine the benefits of additional stand-alone EDS machines to screen checked baggage in place of more labor-intensive ETD machines currently used at more than 300 commercial airports.

To assist TSA in planning for the optimal deployment of checked baggage screening systems, we recommended that TSA systematically evaluate baggage screening needs at airports, including the costs and benefits of installing in-line baggage screening systems at airports that do not yet have in-line systems installed. DHS agreed with our recommendation, stating that TSA has initiated an analysis of deploying in-line checked baggage screening systems and is in the process of formulating criteria to identify those airports that would benefit from an in-line system. DHS also stated that TSA has begun conducting an analysis of the airports that rely heavily on ETD machines as the primary checked baggage screening technology to identify those airports that would benefit from augmenting ETDs with stand-alone EDS equipment.

TSA Is Taking Steps to Enhance Screener Training and Measure Screener Performance

Since we first reported on TSA's passenger screening program in September 2003, TSA has taken a number of steps to expand training available to the screener workforce and to develop performance measures to assess screener performance. With regard to screener training, the President's fiscal year 2006 budget requests $91 million to fully implement TSA's passenger and baggage screener training programs and related workforce development programs at the expected fiscal year 2006 screener workforce level. However, as we reported this time last year, insufficient screener staffing and, at many airports, a lack of high-speed Internet/intranet connectivity have made it difficult for all screeners to receive required training and have access to all courses offered.[8] Specifically, we reported that Federal Security Directors[9] at 5 of the 15 category X airports we visited—during our reviews of passenger and baggage screening—stated that it was difficult, if not impossible, to comply with TSA's recurrent training requirement of 3 hours each week, averaged over a 3-month period.[10] The directors stated that because of

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

[9]Federal Security Directors are responsible for providing day-to-day operational direction for federal security at airports. The Federal Security Director is the ranking TSA authority responsible for the leadership and coordination of TSA security activities at the airport.

[10]TSA classifies the over 450 commercial airports in the United States into one of five security risk categories (X, I, II, III, IV, and V) based on various factors, such as the total number of takeoffs and landings annually, the extent to which passengers are screened at the airport, and other special security considerations. In general, category X airports have the largest number of passenger boardings, and category IV airports have the smallest.

staffing shortages, they were unable to let screeners take required training because it would affect the director's ability to provide adequate screener coverage.

In May 2004, TSA announced a revised allocation of the 45,000 full-time equivalent screeners among the nation's airports in order to provide more appropriate screener coverage. TSA based the allocation on various factors, including forecasted air travel, hours of operation, baggage screening and checkpoint configurations, types of screening equipment deployed, and actual operating experience. In addition, TSA headquarters officials stated that TSA is factoring training requirements into workplace planning efforts, including a new staffing model currently under development.[11] However, it is too soon to determine whether the staffing model will address TSA's ability to provide required training while maintaining adequate coverage for screening operations.[12] The President's request of about $2.7 billion for the screener workforce in fiscal year 2006 represents an increase of about $245 million over last year's enacted budget, but maintains the screener staffing level at the congressionally mandated ceiling of 45,000 full-time equivalent screeners.

The lack of high-speed Internet/intranet connectivity at airport training facilities has also limited screener access to TSA training tools. TSA established its Online Learning Center to provide passenger and baggage screeners with online, high-speed access to training courses. However, effective use of the Online Learning Center requires high-speed Internet/intranet access, which TSA has not been able to provide to all airports. In February 2004, we reported that TSA had provided connectivity to 71 airport locations, including training sites with 927 fully connected training computers, and expected to install high-speed connectivity at up to 81 additional airports by the end of fiscal year 2004. [13]

[11]In May 2003, TSA hired a contractor to develop a staffing model for its screening workforce. TSA officials reported that the model was completed in June 2004, and all airports now have the capability to use the contractors' standalone software. TSA expects to install the software on its intranet by the end of February 2005, thereby providing headquarters with access to the staffing models used at airports.

[12]The Intelligence Reform and Terrorism Prevention Act of 2004 (Pub.L. No. 108-458) requires TSA to develop standards for determining aviation security staffing at commercial airports no later than 90 days after its enactment—December 14, 2004. It also directs GAO to conduct an analysis of these standards, which we will initiate once the standards are developed.

[13]TSA defines a fully connected training computer as one that has the network image installed and is connected to the TSA broadband network.

However, TSA suspended installation of high-speed connectivity at airports in April 2004 when funding was exhausted. Currently, TSA reports that it has provided high-speed connectivity to 120 airports with 1,822 fully connected training computers. TSA plans to continue to distribute new training products using other delivery channels, such as written training materials and CD-ROMs. However, we reported that until TSA provides high-speed connectivity at every airport, screeners at airports without high-speed connectivity will not have access to the full menu of courses available through the Online Learning Center.

The budget request for fiscal year 2006 includes $174 million to complete the installation of high-speed connectivity at the nation's commercial airports. The budget request stated that without these funds, 379 out of 600 (63 percent) of the field sites, including airports, will continue to communicate and provide security-related information over dial-up Internet connections, causing delays and access problems. We believe that the installation of high-speed connectivity at the nation's airports will significantly increase screener access to available training, thereby assisting TSA in strengthening its screening operations. For example, the budget request stated that without these funds, screeners would not have access to training programs such as "Threat of the Day," which allows screeners to stay abreast of the most current security threats.

In addition to training, developing performance measures for TSA's screening program is necessary to assess achievements and make decisions about where to direct performance improvement efforts. In April 2004, we reported that while TSA was taking steps to measure screener performance, it had not collected sufficient data to assess how well screeners performed—particularly with regard to baggage screeners—and had not determined what steps to take to strengthen screener performance.[14] Since then, TSA has gathered additional performance data and has established performance measures and targets for the screening system. We have an ongoing review assessing TSA's efforts in strengthening screener training and measuring performance. This review will address TSA's efforts in developing performance measures to assist in the prioritization of security improvements.

[14]See GAO, *Aviation Security: Private Screening Contractors Have Little Flexibility to Implement Innovative Approaches*, GAO-04-505T (Washington, D.C.: April 22, 2004).

TSA Efforts to Implement a Risk Management Approach for Securing Air Cargo Are Ongoing

TSA's Air Cargo Strategic Plan, completed in November 2003, outlines a threat-based, risk management approach for securing the air cargo transportation system. Specifically, the plan identifies priority actions based on risk, cost, and deadlines. The plan also calls for coordinated efforts in four strategic areas—enhancing shipper and supply chain security, identifying elevated risk cargo through prescreening, identifying technology for performing targeted air cargo inspections, and securing all-cargo aircraft through appropriate facility security measures. In November 2004, TSA published a proposed rule that would implement many of the provisions of the Air Cargo Strategic Plan for enhancing air cargo security.

The President's fiscal year 2006 budget requests $40 million for ensuring the security of air cargo. The $40 million request will support the 200 authorized air cargo inspectors and associated air cargo screening operations initiated during fiscal year 2005. In addition, the request will support the continued development of required programs, training and development of requirements for Indirect Air Carriers,[15] and improvements and maintenance of the Known Shipper[16] and Indirect Air Carrier Program Databases. TSA will also field test the Air Cargo Freight Assessment Program, which will incorporate the Known Shipper and Indirect Air Carrier Program Databases.

TSA's proposed rule for air cargo security describes a number of actions that must be taken before a comprehensive risk management approach can be applied to securing cargo. One of the key components of TSA's risk-based approach for securing air cargo is the development and implementation of a system to screen 100 percent of high-risk cargo. This program, known as the Freight Assessment System, is based on several key components. First, the system will use data on known shippers and indirect air carriers who deliver cargo to air carriers for transport. It is important that this data be complete, accurate, and current, so that shippers about whom relevant security information is known can be distinguished from those shippers about whom there is inadequate security information. Second, the system must incorporate criteria for profiling cargo so that it can identify high-risk cargo that must undergo

[15]An indirect air carrier is an entity, such as a freight forwarder, that engages indirectly in the air transportation of property on passenger aircraft.

[16]Known shippers are entities that have routine business dealings with freight forwarders or air carriers and are thus considered trusted shippers, in contrast to unknown shippers who have conducted limited or no prior business with a freight forwarder or air carrier.

physical screening. Third, effective technology must be deployed to screen cargo identified as high-risk.

TSA is still in the early stages of developing the Freight Assessment System and needs to resolve several issues that could affect the system's development. First, the principal source of data for prescreening is through the use of its Known Shipper Program. However, carriers who collect this information are not currently required to submit data on known shippers for inclusion in TSA's centralized database. In May 2004, a TSA official testified that the known shipper database contained only about one-third of all known shippers. There are also concerns about the relative ease of obtaining known shipper status, and the ability for someone to pose as a known shipper by falsifying or counterfeiting shipping documents used to identify the source as a known shipper. Second, the TSA working group charged with proposing criteria for profiling cargo has not yet reported its recommendations to TSA. Any field testing of the Freight Assessment System will require complete and verified data on known shippers, as well as criteria for evaluating risk. Finally, TSA is in the early stages of identifying and testing air cargo security technologies. For example, it has not yet developed plans outlining when these tests will be completed, or determined whether technologies proven to be effective will be deployed.

In addition, TSA's proposed air cargo security rule estimates the costs of implementing the agency's proposals for enhancing air cargo security at $837 million over a 10-year period. However, industry stakeholders have raised concerns over TSA's projected cost estimates, in part because of the number of air cargo workers the stakeholders estimate to be affected by some of the proposed measures. For example, several stakeholders commented that TSA's cost estimate for conducting the proposed security threat assessments of air cargo workers was low, and that TSA underestimated the number of air cargo workers that would have to undergo an assessment. In addition, air cargo industry stakeholders expressed concerned that they would incur approximately 97 percent of the projected cost of the air cargo security procedures described in the proposed rule. We have an ongoing review evaluating TSA's efforts to implement a risk-based approach to securing air cargo, including TSA efforts to target high-risk cargo, and efforts to identify and test screening technologies.

TSA Has Taken Actions to Strengthen the Security of Commercial Airport Perimeters and Access Controls, but More Work Is Needed

In June 2004, we reported that TSA had taken a variety of actions to evaluate the security of airport perimeters and the controls that limit access into secured airport areas, but had not yet determined how the results of these evaluations could be used to make systemwide improvements.[17] Specifically, TSA has conducted regulatory compliance inspections, covert (undercover) testing of selected security procedures, and vulnerability assessments at selected airports. These evaluations—though not yet complete—have identified perimeter and access control security concerns. For example, TSA identified instances where airport operators failed to comply with existing security requirements, including access control-related regulations. In addition, TSA identified threats to perimeter and access control security at each of the airports where vulnerability assessments were conducted during 2003. In January 2004, TSA temporarily suspended its assessment efforts to conduct higher-priority vulnerability assessments dealing with shoulder-fired missiles. Although TSA plans to begin conducting joint vulnerability assessments with the Federal Bureau of Investigation, it has not yet determined how it will allocate existing resources between its own independent airport assessments and the new joint assessments, or developed a schedule for conducting future vulnerability assessments. Further, TSA has not yet determined how to use the results of its inspections, in conjunction with covert testing and vulnerability assessments results, to enhance the overall security of the commercial airport system.

TSA has also helped some airports enhance perimeter and access control security by providing funds for security equipment, such as electronic surveillance systems. TSA has further initiated efforts to evaluate the effectiveness of security-related technologies, such as biometric identification systems. By December 2003, responsibility for funding most airport security projects had shifted from the Federal Aviation Administration to TSA. As a result, TSA is developing new policies to determine how to review, approve, and prioritize security project funding. However, we reported that TSA has not yet begun to gather data on airport operators' historical funding of security projects and current needs to aid the agency in setting funding priorities.

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

Regarding reducing the potential security risk posed by airport workers, we found that, at the time of our review, TSA had not fully addressed all related requirements mandated by ATSA. For example, TSA required fingerprint-based criminal history records checks and security awareness training for most, but not all, airport workers called for in the act. We also found that TSA had not addressed the act's provision that requires airport vendors with direct access to the airfield and aircraft to develop security programs to address security measures specific to vendor employees. TSA said that expanding requirements for background checks and security awareness training for additional workers and establishing requirements for vendor security programs would be costly to implement.

On the basis of our work, we recommended, and DHS generally agreed, that TSA better justify future decisions on how best to proceed with security evaluations, fund and implement security improvements—including new security technologies—and implement additional measures to reduce the potential security risks posed by airport workers. In July 2004, TSA made several improvements in these areas, through the issuance of a series of security directives, including requiring enhanced background checks and improved access controls for airport employees who work in restricted airport areas.

Continued Partnerships and Risk Assessments Are Needed for Securing General Aviation

The federal and state governments and general aviation industry all play roles in securing general aviation operations. While the federal government provides guidance, enforces regulatory requirements, and provides some funding, the bulk of the responsibility for assessing and enhancing security falls on airport operators. In November 2004, we reported that although TSA has issued a limited threat assessment of general aviation, and the Federal Bureau of Investigation has said that terrorists have considered using general aviation to conduct attacks, a systematic assessment of threats has not been conducted.[18] In addition, we reported that TSA had conducted vulnerability assessments at a small number of general aviation airports, but agency officials stated that conducting these assessments is costly and, therefore, impractical to do for the 19,000 general aviation airports nationwide.

[18]GAO, *General Aviation Security: Increased 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).

TSA intends to implement a risk management approach to better assess threats and vulnerabilities of general aviation aircraft and airports and, as part of this approach, is developing an online vulnerability self-assessment tool to be completed by individual airport managers. However, we found limitations in the use of the self-assessment tool. Further, at the time of our review, these efforts had not been completed, and TSA had not yet developed a plan with specific milestones for implementing the tools and assessments. Without such a plan, it will be difficult for TSA to determine the proper allocation of its resources to the areas of greatest need and to monitor the progress of its efforts.

TSA has also partnered with industry associations to develop security guidelines that enable general aviation airport managers to assess their own vulnerabilities to terrorist attack, and works through industry associations to communicate threat information. However, industry and state aviation officials we spoke with stated that security advisories distributed by TSA were general in nature and were not consistently received. In part this is understandable because, among other things, TSA relies on other federal agencies for threat information. However, we have found that applying risk communication principles—relaying only timely, specific, and actionable information, to the extent possible—provides organizations like TSA with the best opportunity to achieve desired results.

We also found that TSA and the Federal Aviation Administration have taken a number of steps to address security risks to general aviation through regulation and guidance but still face challenges in their efforts to further enhance security. For example, TSA developed regulations governing background checks for foreign candidates for U.S. flight training schools and issued security guidelines for general aviation airports. However, we found limitations in the process used to conduct compliance inspections of flight training schools.

Because of the importance of securing general aviation operations and to help address associated challenges, we recommended, and DHS generally agreed, that TSA take actions to better assess the possibility of terrorists' misuse of general aviation aircraft, better communicate terrorist threat information, and help mitigate security risks to general aviation operations.

TSA Established a Screening Partnership Program but Needs to Finalize Performance Measures

In November 2004, we reported on our preliminary observations of TSA's efforts to establish and implement a Screening Partnership Program, a program through which commercial airports can apply to TSA to use private rather than federal passenger and baggage screeners.[19] Beginning on November 19, 2004, TSA was required by law to begin allowing commercial airports to apply to use private contractors to screen passengers and checked baggage. A federal workforce has performed this function since November 2002, in response to a congressional mandate that the federal government take over screening services from air carriers after the terrorist attacks of September 11, 2001. A 2-year pilot program at five airports testing the effectiveness of private sector screening in a post-September 11 environment was concluded on November 18, 2004.

In assessing TSA's efforts to implement a Screening Partnership Program, we found that TSA had completed or was developing key policies and procedures addressing program implementation and oversight, and was taking steps to communicate with stakeholders by developing informational guidance and soliciting information and suggestions. However, we found that some airport operators, private screening contractors, and aviation industry representatives identified the need for additional information regarding flexibilities airports and contractors would have to manage the program, liability in the event of a terrorist attack, and costs related to program participation.

We also reported that consistent with risk management principles, TSA was developing performance measures to assess the performance of airports participating in the Screening Partnership Program and individual contractors performing the screening services. However, we found that specific performance measures had not yet been finalized and were not scheduled to be completed until mid-2005. TSA officials stated that once developed, performance measures for the Screening Partnership Program will be based on measures already developed by an independent consulting firm for the five airports that participated in the pilot screening program. These measures include how well screeners detect test threat objects, such as guns and knives, during screening operations. TSA also reported that it plans to develop performance measures evaluating how well private screening contractors comply with the terms of their

[19]GAO, *Aviation Security: Preliminary Observations on TSA's Progress to Allow Airports to Use Private Passenger and Baggage Screening Services*, GAO-05-126 (Washington, D.C.: Nov. 19, 2004).

contracts, which they intend to become part of a quality assurance plan. GAO has consistently supported program evaluation—including the development and use of performance measures to measure program outcomes—as an important tool in assessing whether programs are achieving intended goals.

The President's budget request for fiscal year 2006 includes about $161million for the five private contract screening airports. The administration expects contract screening operations to expand beyond the five airports currently using private screening contractors through 2006. To date, one additional airport beyond the five that participated in the pilot program has applied to use private screening contractors. Beginning in May 2005, TSA will begin awarding contracts to private screening contractors. We are continuing to assess TSA's development and implementation of the Screening Partnership Program, to include its development of performance measures to assess screener performance.

TSA Has Begun to Increase Focus on Passenger and Transit Rail Security

We have reported on the security of passenger and transit rail in the past, most recently during testimony before this committee in March 2004.[20] At that time, we stated that following the September 11 terrorist attacks, passenger and freight rail providers implemented new security measures or increased the frequency or intensity of existing activities, including performing risk assessments, conducting emergency drills, and developing security plans. We also reported that—because of a focus on commercial aviation security—TSA initially devoted limited attention to passenger and transit rail security. Since that time, TSA has begun to focus more attention on rail security needs and is in the process of assessing critical passenger rail assets—such as stations, tunnels, and bridges. The Federal Transit Administration also plays a role in rail security, including providing grants for emergency drills and conducting security assessments at the largest transit agencies. The fiscal year 2006 budget requests includes $8 million for rail security to support funding requirements for 100 surface transportation inspectors that will focus primarily on rail security. The budget request identified that the remaining $24 million of the surface transportation budget will support operational funding requirements, the development and implementation of performance-based standard and

[20]GAO, *Rail Security: Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain*, GAO-04-598T (Washington, D.C.: March 23, 2004.)

regulations, vulnerability assessments for critical assets, and security awareness training and exercises.

We are currently reviewing TSA's efforts to strengthen passenger rail and transit security, including determining to what extent threats and vulnerabilities to rail systems have been assessed, what actions have been taken to strengthen security, and the applicability of foreign rail security practices to the U.S. rail system.Our review, among other things, will determine the extent to which federal rail security efforts are consistent with risk management principles to ensure that finite resources are allocated where they are needed most, and that security efforts are being coordinated to help avoid duplication and support integration. Our review will also identify any challenges involved with implementing measures to improve rail security, including practices used by foreign rail systems.

DHS Proposal to Integrate Common Functions Is Commendable, but Existing Challenges Will Need to Be Addressed

DHS's fiscal year 2006 budget request proposes two key changes in DHS's organizational structure that are designed to achieve synergy and avoid duplication of effort. First, DHS proposes to create an Office of Screening Coordination and Operations within the Border and Transportation Security Directorate that would coordinate a comprehensive approach to several ongoing terrorist-related screening initiatives—in immigration; law enforcement; intelligence; counterintelligence; and protection of the border, transportation systems, and critical infrastructure.[21] Specifically, the Office of Screening Coordination and Operations would consolidate nine screening activities, including six that are currently housed within a single TSA office. DHS expects this consolidation to save administrative overhead costs, thereby enabling the department to use those savings toward accomplishing the missions of the programs. In total, DHS is requesting about $847 million for the Office of Screening Coordination and Operations. Table 2 provides the budget request for the 6 screening activities that currently reside within TSA.[22]

[21]The mission of the Office of Screening Coordination and Operations would be to enhance terrorist-related screening through comprehensive, coordinated procedures that detect, identify, track, and interdict people, cargo and conveyances, and other entities and objects that pose a threat to homeland security.

[22]DHS's fiscal year 2006 request for the proposed Office of Screening Coordination and Operations also includes about $390 million for US-VISIT; $7 million for Free and Secure Trade, and $14 million for NEXUS/Secure Electronic Network Rapid Inspection, which are currently part of DHS's Office of Customs and Border Patrol.

Table 2: Fiscal Year 2006 Budget Request for TSA Activities DHS Has Proposed to Transfer to the Office of Screening Coordination and Operations

Program	FY 2006 budget request ($000)
Secure Flight (including crew vetting)	$ 94,294
Credentialing Startup	20,000
Discretionary Fee Funded: Transportation Worker Identification Credential	244,722
Discretionary Fee Funded: Registered Traveler	22,500
Discretionary Fee Funded: HAZMAT	44,165
Mandatory Fee Funded: Alien Flight School Checks	10,000
Total	**$435,681**

Source: DHS.

DHS identified 11 goals in creating the Office of Screening Coordination and Operations:

- enable consistent, effective, and efficient day-to-day operations through the application of standards and use of common services;
- assist in the development of policy for DHS-wide screening and credentialing programs;
- create an integrated business strategy for DHS screening and credentialing programs that enhances security, facilitates travel, and safeguards privacy;
- reduce redundancy and close mission and technological gaps;
- manage investments of screening and credentialing programs to ensure efficient use of assets;
- remove technological barriers to sharing screening information within DHS;
- enable consistent status reporting of major screening and credentialing programs;
- ensure consistent acquisition/contracting and program management processes/disciplines are applied;
- establish a central clearinghouse to administer registered traveler programs and worker credentialing programs;
- deliver clear and consistent messages to domestic and foreign travelers and workers for increased compliance; and
- work with other federal agencies to improve and coordinate screening standards.

Second, DHS is proposing to consolidate its R&D efforts inside its Science and Technology Directorate.[23] This office will house the current R&D activities that are currently spread across four DHS component agencies—TSA, U.S. Coast Guard, Customs and Border Patrol, and Information Analysis and Infrastructure Protection Directorates. The existing TSA R&D program consists of research and development (Transportation Security Laboratory),[24] next-generation explosive detection systems, and air cargo research, and received a total of $178 million in fiscal year 2005 appropriations.[25] By consolidating these and other R&D programs under a single office, DHS is seeking to maximize the efficiency and effectiveness of its R&D efforts to allow the components to focus on their operational missions and eliminate duplicate management infrastructure. DHS's fiscal year 2006 budget request includes $1.4 billion for R&D.

We applaud DHS's efforts to achieve efficiencies and cost savings, leverage resources and technology, and improve internal coordination and operations. As DHS works toward consolidating screening functions and initiatives within the Office of Screening Coordination and Operations, and the R&D functions within the Science and Technology Directorate, it will be important for DHS to define the interrelationships and commonalities among these programs, explicitly define roles and responsibilities, and identify data needs. Additionally, DHS will need to address the existing challenges that have been identified regarding the programs these offices will absorb. While these organizational changes should assist DHS in providing a solid foundation from which to manage and oversee its screening, credentialing, and R&D efforts, restructuring alone will not resolve all existing challenges or ensure the successful integration and achievement of DHS's goals. We have recently reported on challenges DHS and TSA are facing with regard to some of these programs, including Secure Flight, the Transportation Worker Identification Credential, and research and development activities. The sections below describe the challenges we identified.

[23]The Homeland Security Act of 2002 states that DHS is responsible for coordinating and integrating all research, development, demonstration, testing, and evaluation activities of the Department. Pub.L. No. 107-296, § 302(12).

[24]TSA's Transportation Security Laboratory performs research and development related to civil transportation security.

[25]The budget proposal consolidates the bulk of TSA's research and development programs into the Science and Technology Directorate, resulting in a transfer of $109 million. TSA will retain $23 million for operational research and development activities in FY 2006.

TSA Is in Early Stages of Testing and Implementing the Secure Flight Passenger Prescreening System

One challenge the proposed Office of Screening Coordination and Operations will face immediately is the continued development of a system to prescreen domestic airline passengers. The prescreening of passengers—that is, determining whether airline passengers pose a security risk before they reach the passenger screening checkpoint—is used to focus security attention on those passengers representing the greatest potential threat. Since the late 1990s, passenger prescreening has been conducted using the Computer-Assisted Passenger Prescreening System (CAPPS I). This system, operated by air carriers, compares passenger information against CAPPS I rules as well as a government-supplied watch list that contains the names of known or suspected terrorists.[26]

In the wake of September 11, concerns were raised over the effectiveness of CAPPS I. In 2002, TSA began developing a second-generation computer-assisted passenger prescreening system, known as CAPPS II, which was intended to provide a more effective and efficient way to prescreen airline passengers. However, the development of CAPPS II faced a number of significant delays and challenges. As we reported in February 2004, key activities in the development of CAPPS II were delayed, complete plans identifying system functionality were not established, and TSA was behind schedule in testing and developing initial increments of the system.[27] Further, we found that TSA had not yet fully addressed seven of the eight issues identified by Congress as key areas of interest, such as privacy concerns, passenger redress, and system oversight. We further reported that TSA faced challenges in obtaining the international cooperation needed to obtain passenger data, managing the expansion of the program's mission beyond its original purpose, and ensuring that identify theft—in which an individual poses as and uses information of another individual—cannot be used to negate the security benefits of the system.

Moreover, in July 2004, the 9/11 Commission advised that improvements to the passenger prescreening system are required, noting that the watch lists used by the air carriers for the current prescreening system, CAPPS I, do not include all terrorists or terrorism suspects because of concerns about

[26]CAPPS I rules are behavioral characteristics associated with the way an airline ticket is purchased.

[27]GAO, *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385 (Washington, D.C.: February 12, 2004).

sharing intelligence information with private firms and foreign countries.[28] The 9/11 Commission stated that passenger prescreening should be performed by TSA and should use the larger consolidated watch list data maintained by the federal government. As a result of these problems and challenges, as well as widespread concerns with CAPPS II by Congress, the public, and other key stakeholders, DHS terminated the CAPPS II program and in August 2004 announced that it would develop a new passenger prescreening program called Secure Flight.

Under Secure Flight, TSA will take over, from commercial airlines, the responsibility for checking passenger information against terrorist watch lists and the CAPPS I rules. TSA expects that Secure Flight, once implemented, will provide a number of benefits over the current airline-operated system. For example, TSA expects that Secure Flight will be more effective than CAPPS I in identifying terrorists because it will utilize an expanded watch list with more information than is currently available to air carriers. TSA also believes Secure Flight will reduce the number of passengers mistakenly identified as being on a terrorist watch list as compared with the current system. TSA is currently testing the ability of Secure Flight to perform watch list matching and applying CAPPS I rules.[29] TSA expects that this phase of testing will be completed later this month. In addition, TSA plans to test the feasibility of using commercial data to improve the ability of Secure Flight to more accurately verify passenger identity. TSA expects to complete commercial data testing in early April 2005.[30] On the basis of these test results, TSA plans to make policy decisions regarding the use of commercial data as part of Secure Flight. TSA also plans subsequently to test additional functionality and the operations of Secure Flight before implementation, regardless of whether it incorporates the use of commercial data as part of Secure Flight. At the conclusion of testing, TSA expects to implement Secure Flight with one or two air carriers in August 2005.

Although TSA reported that it spent approximately $100 million on the development of CAPPS II, TSA considers much of that cost to be

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

[29]In order to obtain data for testing, TSA issued an order in November 2004 requiring domestic airlines to provide passenger records for the month of June 2004.

[30]We have ongoing work assessing TSA's testing of commercial data and expect to issue a report later this month.

applicable to Secure Flight. This is because Secure Flight will leverage certain capabilities that had been developed for the CAPPS II program, such as the system infrastructure used to match passenger information against terrorist watch lists. However, in developing Secure Flight, TSA modified the CAPPS II infrastructure to remove certain features that were not authorized for Secure Flight. For fiscal year 2005, TSA was allocated $35 million for the development of Secure Flight. The President's fiscal year 2006 budget request includes approximately $94 million for Secure Flight development and implementation as well as crew vetting.[31] This represents an increase of approximately $46 million for Secure Flight and approximately $3 million for crew vetting. These funds are intended to support continued testing, information systems, connectivity to airlines, and daily operations.

As mandated by the fiscal year 2005 Homeland Security Appropriations Act (Public Law 108-334, Section 522), as well as in response to congressional requests, we are currently conducting a review of the Secure Flight program.[32] Our review will highlight four key areas: (1) the status of Secure Flight's development and implementation, (2) any challenges to the system's effective implementation and operation, (3) processes in place for system oversight and program management, and (4) efforts to minimize the impact of Secure Flight on passengers and to protect passenger rights. As part of this review, we will examine the future costs associated with the development and implementation of Secure Flight. We will also determine if TSA has addressed the weaknesses identified in our February 2004 report on CAPPS II. We will issue a report discussing the results of our review by March 28, 2005.

[31]The proposal to create the new Office of Screening Coordination and Operations would combine two screening programs that will use the same system infrastructure—Secure Flight and crew vetting. The crew vetting program matches names of aircraft pilots and flight and cabin crew against terrorist watch lists. Currently, these programs are run by the Office of Transportation Vetting and Credentialing.

[32]This review is separate from our ongoing work assessing TSA's commercial data testing efforts.

TSA Faces Planning Challenges in Moving Forward with the Transportation Worker Identification Credential

The Office of Screening Coordination and Operations will also need to address the challenges TSA has faced in developing a Transportation Worker Identification Credential (TWIC). The TWIC program is intended to improve security by establishing an integrated, credential-based, identity management program for higher risk transportation workers requiring unescorted access to secure areas of the nation's transportation system. TSA expects that the Office of Screening Coordination and Operations will leverage separate screening processes within TWIC, such as in establishing watchlist checks on transportation workers and establishing access interoperability with transportation companies, and apply those practices to other screening activities.

In December 2004, we reported on TSA's efforts to issue a worker identification card that uses biometrics, such as fingerprints, to control access to secure areas of ports or ships.[33] We found that three main factors caused TSA to miss its initial August 2004 target date for issuing maritime worker identification cards: (1) TSA officials had difficulty obtaining timely approval of the prototype test from DHS because of competition for executive-level attention and agency resources, (2) extra time was required to work with DHS and Office of Management Budget officials to identify additional data to be collected for cost-benefit and alternative analyses, and (3) additional work was required to assess the capabilities of various card technologies to determine which technology was most appropriate for controlling access in seaports. Because of program delays, some port facilities, recognizing an immediate need to enhance access control systems, are proceeding with plans for local or regional identification cards that may require additional investment in order to make them compatible with the TWIC system. Accordingly, delays in the program may affect enhancements to port security and complicate stakeholder's efforts in making wise investment decisions regarding security infrastructure.

We also identified additional challenges that DHS will face as it moves forward with developing and operating the TWIC program, such as developing regulations that identify eligibility requirements for the card and instituting a comprehensive plan for managing the project. A documented comprehensive project plan will assist DHS in achieving mutual understanding, commitment, and performance of individuals,

[33]GAO, *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, GAO-05-106 (Washington, D.C.: Dec. 10, 2004).

groups, and organizations that must execute or support the plan. Without such a plan—which is an established industry best practice for project planning and management—the program's schedule and performance is placed at higher risk. For example, additional delays could occur unless involved parties agree on efforts guiding the remainder of the project, stakeholder responsibilities, and associated deadlines. Additionally, without a plan to guide the cost-benefit and alternatives analyses—another industry best practice—risk is increased that DHS may not sufficiently analyze the feasibility of various approaches to issuing the card, an analysis needed to make informed decisions regarding the program.[34] On the basis of our work, we recommended, and DHS generally agreed, that TSA employ industry best practices for project planning and management by developing a comprehensive project plan for managing the program and specific detailed plans for risk mitigation and cost-benefit and alternatives analyses. As DHS moves forward in developing TWIC, it will be important that it incorporates these best practices to help address the challenges it faces in developing and implementing a maritime worker identification card.

DHS's fiscal year 2006 budget request includes about $245 million for TWIC. This amount is to cover the costs of personnel, contractors, equipment maintenance, software and license updates, background checks, fingerprint processing, and adjudication of results. DHS estimated that the $245 million will enable it to distribute roughly 2 million TWICs to transportation security workers needing access to high-risk areas of the transportation system by the end of fiscal year 2006. Additionally, DHS is seeking authority to recover these costs in their entirety through fees charged to the applicants.

TSA is also exploring the cost-effectiveness of two other program alternatives: (1) a federal approach: a program wholly designed, financed, and managed by the federal government, and (2) a decentralized approach: a program requiring ports and port facilities to design, finance, and manage programs to issue identification cards. In February 2005, TSA officials stated that they do not expect to make a decision on which of the three alternatives to implement—the federal, decentralized, or TWIC

[34]Best practices indicate that plans for activities such as cost-benefit and alternatives analyses should be developed to help facilitate data collection and analysis. These plans typically describe, among other things, the data to be collected, the source of these data, and how the data will be analyzed. Such plans are important to guide needed data analysis as well as prevent unnecessary data collection, which can be costly.

program—until later in 2005. Officials stated that whichever approach is selected will be known as TWIC and will meet legislative requirements.

Further Planning, Risk Assessment, and Coordination Needed to Focus R&D Efforts

As DHS moves forward in integrating its R&D functions into a single office—a commendable goal—it will be important for the department to resolve the existing challenges facing its various R&D programs. Researching and developing technologies to detect, prevent, and mitigate terrorist threats is vital to enhancing the security of the nation's transportation system. In September 2004, we reported that TSA and DHS have made some progress in managing transportation security R&D programs according to applicable laws and R&D best practices.[35] However, we found that their efforts were incomplete in several areas, including preparing strategic plans for R&D efforts that contain measurable objectives, preparing and using risk assessments to select and prioritize R&D projects, and coordinating with stakeholders. We also found that TSA and DHS delayed several key R&D projects and lacked both estimated deployment dates for the vast majority of their R&D projects and adequate databases to effectively manage their R&D portfolios.

The Homeland Security Act requires DHS, through its Science and Technology Directorate, to prepare a strategic plan that identifies goals and includes annual measurable objectives for coordinating the federal government's civilian efforts in developing countermeasures to terrorist threats. Similarly, the National Academy of Sciences has stated that research programs should be described in strategic and performance plans and evaluated in performance reports. We are encouraged that TSA and DHS have prepared strategic plans for their agencies, and that TSA has prepared a strategic plan for its R&D program. However, we found that these plans do not contain measurable objectives for tracking the progress of R&D efforts. We recommended that TSA and DHS complete strategic plans containing measurable objectives for their transportation security R&D programs. According to DHS officials, the department is preparing a separate strategic plan for its R&D program that will include more specific goals and measurable objectives. DHS also stated that the Science and Technology Directorate's strategic planning process will include

[35]GAO, *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).

(1) determining strategic goals for the next 5 years, threats, and vulnerabilities, and (2) developing a list of prioritized projects for fiscal years 2005 through 2010.

In consolidating its R&D functions, it will also be important for DHS to use risk management principles in making R&D funding decisions, as required by ATSA.[36] Although both TSA and DHS have established processes to select and prioritize R&D projects that include risk management principles, they have not yet completed vulnerability and criticality assessments, which we have identified as key elements of a risk management approach, for all modes of transportation.[37] In the absence of completed risk assessments, TSA and DHS officials report basing funding decisions on other factors—such as available threat intelligence, expert judgment, and information about past terrorist incidents. TSA officials further stated that TSA's Chief Technology Officer receives daily intelligence briefings and that the agency uses threat information to select R&D projects to pursue. However, officials stated that they do not use formal threat assessments to make R&D decisions. In addition, the DHS Inspector General reported in March 2004 that although many senior officials agreed that DHS's Science and Technology and the Information Analysis and Infrastructure Protection Directorates should closely coordinate, staff below them were not actively involved in sharing terrorist threat information or using the information to form the basis for selecting new homeland security technologies. On the basis of our work, we recommended, and DHS generally agreed, that TSA and DHS use the results of risk assessments to help select and prioritize their R&D efforts.

In moving forward with the proposed integration of R&D functions, DHS will also need to enhance its efforts to coordinate with other federal agencies with respect to transportation security R&D, and reach out to industry stakeholders. ATSA and the Homeland Security Act require DHS to coordinate its efforts with those of other government agencies, in part to reduce duplication and identify unmet needs. Similarly, R&D best practices identify the importance of stakeholder coordination in

[36]Pub.L. No. 107-71, § 112(b)(1)(B). Additionally, under the Homeland Security Act, DHS is required to establish R&D priorities for detecting, preventing, protecting against, and responding to terrorist attacks (Pub.L. No. 107-296, § 302(5)(B)), and to prepare comprehensive assessments of the vulnerabilities of the nation's key resources and critical infrastructure sectors, one of which is transportation (Pub.L. 107-296, § 201(d)(2)).

[37]GAO, *Homeland Security: Key Elements of a Risk Management Approach*, GAO-02-150T (Washington, D.C.: Oct. 12, 2001).

identifying R&D needs. For TSA and DHS to select the best technologies to enhance transportation security, it is important that they have a clear understanding of the R&D projects currently being conducted, both internally and externally. During our review, we found limited evidence of coordination between TSA and DHS, or between these agencies and other federal agencies, such as the Department of Transportation. Without such coordination, DHS raises the risk that its R&D resources will not be effectively leveraged and that duplication may occur. Further, most transportation industry association officials we interviewed stated that TSA and DHS had not coordinated with them to obtain information on their security R&D needs. We recommended, and officials generally agreed, that TSA should develop a process with the Department of Transportation to coordinate transportation security R&D, such as a memorandum of agreement identifying roles and responsibilities, and share this information with transportation stakeholders.

DHS will also need to address several additional challenges while moving forward in consolidating its R&D functions into a single office, including managing delays in key R&D projects, better estimating deployment dates, and conducting better tracking of its R&D portfolio. During our review, we found that progress on some R&D projects was delayed in fiscal year 2003 when TSA transferred about $61 million, more than half of its $110 million R&D appropriation, to support operational needs, such as personnel cost for screeners. As a result, TSA delayed several key R&D projects related to checked baggage screening, checkpoint screening, and air cargo security. For example, TSA delayed the development of a device to detect weapons, liquid explosives, and flammables in containers found in carry-on baggage or passengers' effects, as well as the development and testing of a walk-through portal for detecting traces of explosives on passengers. We also found that although many of TSA's projects were in later phases of development, the agency had not estimated deployment dates for 133 of the 146 projects that it funded in fiscal years 2003 and 2004. While we recognize that deployment dates are not always predictable, we generally believe that R&D program managers should estimate deployment dates for projects that are beyond the basic research phase because deployment dates can serve as goals that the managers can use to plan, budget, and track the progress of projects. We also found that TSA and DHS did not have adequate databases to monitor and manage the spending of the hundreds of millions of dollars that Congress had appropriated for R&D. For example, for the 146 projects that it funded in 2003 and 2004, TSA was not able to provide us information on anticipated deployment dates for 91 percent, the current phase of development for 49 percent, and the amounts obligated and budgeted for 8 percent that were appropriated tens

of millions of dollars in both fiscal years 2003 and 2004. We recommended that TSA and DHS develop a database to provide accurate, complete, current, and readily accessible project information for monitoring and managing their R&D portfolios, and a vehicle for communicating R&D need with the transportation industry. In September 2004, DHS stated that TSA had developed a system to track R&D projects' goals and milestones, acquisition, funding, testing, and deployment information.

Concluding Observations

DHS and TSA have undertaken numerous initiatives to strengthen transportation security, particularly in aviation, and their efforts should be commended. Meeting the congressional mandates to screen passengers and checked baggage alone was a tremendous challenge—yet TSA successfully hired and deployed a federal screening workforce of over 40,000 and deployed equipment to screen checked baggage for explosives at over 400 commercial airports nationwide. In our previous work addressing transportation security, we identified future actions that TSA should take to enhance security within and across all modes of transportation. Throughout the course of this work, one theme consistently surfaced—the need for TSA to fully utilize and integrate a risk management approach into its decision making processes. Our work has shown—in homeland security and in other areas—that a comprehensive risk management approach can help inform decision makers in allocating finite resources to the areas of greatest need. We are encouraged that the President's fiscal year 2006 budget request discusses TSA's plans to implement a risk management approach in focusing its resources related to transportation security. However, we recognize that fully integrating a risk management approach into decision making processes is challenging for any organization. Further, in order to fully apply this approach, TSA must also address the challenges we have identified in our work related to program planning, risk assessments, and implementation and monitoring. Without rigorous planning and prioritization, and knowledge of the effectiveness of their transportation security programs, DHS and TSA cannot be sure that they are focusing their resources on the areas of greatest need, are addressing the most critical security requirements, and are ensuring the most efficient utilization of its resources.

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

Contact Information

For further information on this testimony, please contact Cathleen A. Berrick at (202) 512-3404.

Individuals making key contributions to this testimony included David Alexander, Chan My J Battcher, Seto J. Bagdoyan, J. Michael Bollinger, Lisa Brown, Kevin Copping, Christine Fossett, John Hansen, Adam Hoffman, Christopher M. Jones, Christopher Keisling, Noel Lance, Thomas Lombardi, Lisa Shibata, and Maria Strudwick.

Related GAO Products Released Since September 11, 2001

Aviation Security: Preliminary Observations on TSA's Progress to Use Private Passenger and Baggage Screening Services, GAO-05-126. Washington, D.C.: November 19, 2004.

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

Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security. GAO-04-838. Washington, D.C.: June 30, 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.

Transportation Security Administration: High-Level Attention Needed to Strengthen Acquisition Function. GAO-04-544. Washington, D.C.: May 28, 2004.

Aviation Security: Private Screening Contractors Have Little Flexibility to Implement Innovative Approaches. GAO-04-505T. Washington, D.C.: April 22, 2004.

Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection. GAO-04-557T. March 31, 2004.

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

Rail Security: Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain. GAO-04-598T. Washington, D.C.: March 23, 2004.

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.: February 13, 2004.

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

Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers. GAO-04-325T. Washington, D.C.: December 16, 2003.

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

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

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

Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain. GAO-03-1155T. Washington, D.C.: September 9, 2003.

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

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

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

Rail Safety and Security: Some Actions Already Taken to Enhance Rail Security, but Risk-based Plan Needed. GAO-03-435. Washington, D.C.: April 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 Plan to Build a Results-Oriented Culture. GAO-03-190 Washington, D.C.: January 17, 2003.

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

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

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

Aviation Security: Registered Traveler Program Policy and Implementation Issues. GAO-03-253. Washington, D.C.: November 22, 2002.

Combating Terrorism: Actions Needed to Improve Force Protection for DOD Deployments through Domestic Seaports. GAO-03-15. Washington, D.C.: October 22, 2002.

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

Mass Transit: Challenges in Securing Transit Systems. GAO-02-1075T. Washington, D.C.: September 18, 2002.

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

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

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

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

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

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

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

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

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548