



Testimony

Before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EST
Thursday, February 28, 2008

AVIATION SECURITY

Transportation Security Administration Has Strengthened Planning to Guide Investments in Key Aviation Security Programs, but More Work Remains

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

and

Gregory C. Wilshusen, Director
Information Security Issues





Highlights of [GAO-08-456T](#), a testimony before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives

Why GAO Did This Study

Transportation Security Administration (TSA) funding for aviation security has totaled about \$26 billion since fiscal year 2004. This testimony focuses on TSA's efforts to secure the commercial aviation system through passenger screening, air cargo, and watch-list matching programs, and challenges remaining in these areas. GAO's comments are based on GAO products issued between February 2004 and April 2007, including selected updates in February 2008. This testimony also addresses TSA's progress in developing the Secure Flight program, based on work conducted from August 2007 to January 2008. To conduct this work, GAO reviewed systems development, privacy, and other documentation, and interviewed Department of Homeland Security (DHS), TSA, and contractor officials.

What GAO Recommends

GAO has made recommendations to DHS in prior reports to strengthen screening operations and air cargo security. DHS generally concurred with our recommendations and is making progress in implementing them. GAO is making new recommendations to DHS to incorporate best practices in Secure Flight cost and schedule estimates; fully implement the program's risk management, testing, and information security requirements; and consider additional performance measures to evaluate redress processes. DHS and TSA generally agreed with GAO's recommendations.

To view the full product, including the scope and methodology, click on [GAO-08-456T](#). For more information, contact Cathleen Berrick at (202) 512-3404 or berrickc@gao.gov.

AVIATION SECURITY

Transportation Security Administration Has Strengthened Planning to Guide Investments in Key Aviation Security Programs, but More Work Remains

What GAO Found

DHS and TSA have undertaken numerous initiatives to strengthen the security of the nation's commercial aviation system, including actions to address many recommendations made by GAO. TSA has focused its efforts on, among other things, more efficiently allocating, deploying, and managing the Transportation Security Officer (TSO) workforce—formerly known as screeners; strengthening screening procedures; developing and deploying more effective and efficient screening technologies; strengthening domestic air cargo security; and developing a government operated watch-list matching program, known as Secure Flight. Specifically, TSA developed and implemented a Staffing Allocation Model to determine TSO staffing levels at airports that reflect current operating conditions, and proposed and implemented modifications to passenger checkpoint screening procedures based on risk information. However, GAO reported that some assumptions in TSA's Staffing Allocation Model did not accurately reflect airport operating conditions, and that TSA could improve its process for evaluating the effectiveness of proposed procedural changes. In response, TSA developed a plan to review Staffing Allocation Model assumptions and took steps to strengthen its evaluation of proposed procedural changes. TSA has also explored new passenger checkpoint screening technologies to better detect explosives and other threats and has taken steps to strengthen air cargo security, including conducting vulnerability assessments at airports and compliance inspections of air carriers. However, TSA has not developed an inspection plan that included performance goals and measures to determine whether air carriers transporting cargo into the United States were complying with security requirements. In response to GAO's recommendations, TSA has since established a working group to strengthen its compliance activities. Finally, TSA has instilled more discipline and rigor into Secure Flight's systems development, including preparing key documentation and strengthening privacy protections.

While these efforts should be commended, GAO has identified several areas that should be addressed to further strengthen aviation security. For example, TSA has made limited progress in developing and deploying checkpoint technologies due to planning and management challenges. Further, TSA continues to face some program management challenges in developing Secure Flight. Specifically, TSA has not (1) developed program cost and schedule estimates consistent with best practices; (2) fully implemented its risk management plan; (3) planned for system end-to-end testing in test plans; and (4) ensured that information security requirements are fully implemented. If these challenges are not addressed effectively, the risk of the program not being completed on schedule and within estimated costs is increased, and the chances of it performing as intended are diminished. DHS and TSA lack performance measures to fully evaluate the effectiveness of current processes for passengers who apply for redress due to inconveniences experienced during the check-in and screening process. Without such measures, DHS and TSA lack a sound basis to monitor the effectiveness of the redress process.

Mr. Chairman and Members of the Subcommittee:

We appreciate the opportunity to participate in today's hearing to discuss the security of our nation's aviation system. The Transportation Security Administration (TSA) was established in 2001 with the mission to protect the transportation network while also ensuring the free movement of people and commerce. Since its inception, TSA has focused much of its efforts on aviation security, and has developed and implemented a variety of programs and procedures to secure commercial aviation. To implement these efforts, TSA funding for aviation security has totaled about \$26 billion since fiscal year 2004. Other parties also play a role in securing commercial aviation, including air carriers that are responsible for screening air cargo, among other things, and the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T), which is responsible for the research and development of aviation security technologies. In carrying out its broader homeland security responsibilities, DHS faces the daunting challenge of determining how to allocate its finite resources within the aviation system and across all sectors to address threats and strengthen security.

Our testimony today focuses on TSA's efforts to ensure the security of the following key areas of the commercial aviation system, which represents about \$4.5 billion of the \$6.0 billion President's fiscal year 2009 budget request for aviation security: 1) screening operations, including transportation security officer (TSO) and private screener allocations, and checkpoint screening technologies; 2) air cargo; and 3) and passenger watch-list matching. In particular, we will address the numerous efforts TSA has taken or plans to take to strengthen security in these areas and the challenges that remain.

Our comments are based on GAO reports and testimonies issued between February 2004 and April 2007 addressing the security of the nation's aviation system, including selected updates to this work conducted in February 2008. Our comments are also based on the results from our recently completed work assessing the status of TSA's development of the Secure Flight program, conducted in response to the Implementing Recommendations of the 9/11 Commission Act of 2007.¹ This statement will address the following issues raised by the mandate: (1) overall progress made in strengthening the Secure Flight program, including

¹ Pub. L. No. 110-53, § 1605(b), 121 Stat. 266, 481-82 (2007).

privacy protection issues and coordination of international and domestic watch-list matching functions, (2) development of Secure Flight's cost and schedule estimates, (3) efforts made in Secure Flight's system development including risk management, end-to-end testing, and information security, and (4) DHS and TSA's efforts to evaluate redress. We conducted this mandated review from August 2007 to January 2008. For our review, we interviewed officials from the Secure Flight program and Customs and Border Protection and reviewed relevant laws and regulations and program management and planning documents. We conducted these performance audits in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Summary

DHS and TSA have undertaken numerous initiatives to strengthen the security of the nation's commercial aviation system and more effectively guide program investments, including steps to address many of our prior recommendations. Meeting the statutory mandates to screen airline passengers and 100 percent of checked baggage alone was a tremendous challenge. TSA has since turned its attention to, among other things, to more efficiently allocating, deploying, and managing the TSO—formerly known as screeners—workforce; strengthening screening procedures; developing and deploying more effective and efficient screening technologies; strengthening air cargo security; and developing a government operated watch-list matching program, known as Secure Flight. More specifically, DHS and TSA have, among other things, developed and implemented a Staffing Allocation Model to determine TSO staffing levels at airports that reflect current operating conditions, and provided TSOs with additional training intended to enhance the detection of threat objects, particularly improvised explosive devices. TSA also proposed and implemented modifications to passenger checkpoint screening procedures based on risk (threat and vulnerability) information, while considering efficiency and customer service needs. TSA also explored new passenger checkpoint screening technologies to enhance the detection of explosives and other threats. Further, TSA took steps to strengthen air cargo security, such as conducting vulnerability assessments at several domestic airports, revising air cargo screening exemptions, and conducting inspections of air carriers to ensure that they are complying with existing security requirements. Finally, TSA has instilled more discipline and rigor into Secure Flight's development and

implementation since we last reported on the program in February 2007, including preparing key systems development documentation and strengthening privacy protections.

While these efforts should be commended, we have reported on several areas in which TSA could do more to strengthen aviation security. For example, in our previous work, we reported that some assumptions in TSA's Staffing Allocation Model did not accurately reflect airport operating conditions. We recommended that TSA establish a formal, documented plan for reviewing all of the model assumptions on a periodic basis. TSA agreed with our recommendation and, in December 2007, developed a Staffing Allocation Model Rates and Assumption Validation Plan that the agency will use to review and validate model assumptions. In addition, we reported that TSA could improve its process for evaluating the effectiveness of proposed changes to passenger screening procedures. For example, while in some cases TSA tested proposed modifications to passenger checkpoint screening procedures before they were implemented to help determine whether the changes would achieve their intended purposes, we found that TSA's data collection and analyses could be strengthened. DHS generally agreed with our findings and recommendations and TSA has taken steps to implement them. We also testified that limited progress has been made in developing and deploying checkpoint technologies due to planning and management challenges. For example, we reported that TSA made limited progress in fielding explosives detection technology at passenger screening checkpoints in part due to challenges DHS S&T and TSA previously faced in coordinating research and development efforts. We further reported that TSA halted the deployment of one technology due to high installation and maintenance costs. With respect to air cargo, we reported that while TSA conducted a variety of compliance inspections to determine whether air carriers or indirect air carriers—entities that consolidate air cargo for delivery and transport—were complying with TSA security requirements, and had begun to analyze the results of these inspections, it has not developed an inspection plan that included performance goals and measures to determine the extent to which air carriers transporting cargo into the United States were complying with security requirements. While TSA has made considerable progress in the development and implementation of Secure Flight, it has not fully addressed program management issues including (1) developing cost and schedule estimates consistent with best practices, (2) fully implementing its risk management plan, (3) developing a comprehensive testing strategy, and (4) ensuring that information security requirements are fully implemented. If these challenges are not addressed effectively, the risk of the program not being completed on schedule and within estimated costs is increased, and the chances of it

performing as intended are diminished. Also, DHS and TSA lack performance measures to fully evaluate the effectiveness of current processes for passengers who apply for redress due to inconveniences experienced during the check-in and screening processes. Having such measures will allow the program to fully measure all of its priorities and make future adjustments to the program.

To strengthen TSA's development and implementation of the Secure Flight program, we are making recommendations to DHS to incorporate best practices in the Secure Flight program and to fully implement the program's risk management plan and information security requirements and develop a comprehensive testing strategy. We are also making a recommendation to DHS and TSA to develop additional performance measures for their current redress process. We provided a draft of information included in this statement related to our recently completed work on Secure Flight to DHS and TSA for review and comment. In commenting on this information, DHS and TSA generally agreed with our recommendations.

Background

With the passage of the Aviation and Transportation Security Act (ATSA) in November 2001, TSA assumed responsibility for civil aviation security from the Federal Aviation Administration and for passenger and checked baggage screening from air carriers.² As part of this responsibility, TSA oversees security operations at the nation's more than 400 commercial airports, including establishing requirements for passenger and checked baggage screening and ensuring the security of air cargo transported to, from, and within the United States. In addition, TSA has operational responsibility for conducting passenger and checked baggage screening at most airports, and has regulatory, or oversight, responsibility, for air carriers who conduct air cargo screening. While TSA took over responsibility for passenger checkpoint and baggage screening, air carriers have continued to conduct passenger watch-list matching in accordance with TSA requirements, which includes the process of matching passenger information against federal watch-list data before flights depart. TSA is currently developing a program to take over this responsibility from air carriers for passengers on domestic flights, and plans to assume from the U.S. Customs and Border Protection (CBP) the pre-departure name-matching function for passengers on international flights traveling to or from the United States.

²See Pub. L. No. 107-71, 115 Stat. 597 (2001).

Airline Passenger and Checked Baggage Screening

One of the most significant changes mandated by ATSA was the shift from the use of private-sector screeners to perform airport screening operations to the use of federal screeners (now referred to as TSOs). Prior to ATSA, passenger and checked baggage screening had been performed by private screening companies under contract to airlines. ATSA established TSA and required it to create a federal workforce to assume the job of conducting passenger and checked baggage screening at commercial airports. The federal screener workforce was put into place, as required, by November 2002.³

Passenger screening is a process by which personnel authorized by TSA inspect individuals and property to deter and prevent the carriage of any unauthorized explosive, incendiary, weapon, or other dangerous item into a sterile area or onboard an aircraft.⁴ Passenger screening personnel must inspect individuals for prohibited items at designated screening locations. The four passenger screening functions are X-ray screening of property, walk-through metal detector screening of individuals, hand-wand or pat-down screening of individuals, and physical search of property and trace detection for explosives. Typically, passengers are only subjected to X-ray screening of their carry-on items and screening by the walk-through metal detector. Passengers whose carry-on baggage alarms the X-ray machine, who alarm the walk-through metal detector, or who are designated as selectees—that is, passengers selected by the Computer Assisted Passenger Pre-Screening System (CAPPS) or other TSA-approved processes to designate passengers for additional screening—are screened by hand-wand or pat-down and have their carry-on items either screened for explosives traces or physically searched.⁵

³ATSA further required TSA to allow airports to apply to opt-out of federal screening and to use private screeners under contract with TSA. *See* 49 U.S.C. § 44920. Ten airports and 1 heliport currently have screening operations conducted by private screening contractors under TSA's Screening Partnership Program.

⁴Sterile areas are located within the terminal where passengers are provided access to boarding aircraft. Access to these areas is controlled by TSOs (or by non-federal screeners at airports participating in the Screener Partnership Program) at checkpoints where they conduct physical screening of individuals and their carry-on baggage for weapons and explosives.

⁵CAPPS identifies passengers for secondary screening based on certain travel behaviors reflected in their reservation information that are associated with threats to aviation security, as well as through a random selection of passengers. At some airports, some passengers may also be screened by walking through an explosives trace portal—a machine that detects trace amounts of explosives on persons.

Checked baggage screening is a process by which authorized security screening personnel inspect checked baggage to deter, detect, and prevent the carriage of any unauthorized explosive, incendiary, or weapon onboard an aircraft. Checked baggage screening is accomplished through the use of explosive detection systems⁶ or explosive trace detection systems,⁷ and through the use of approved alternative means, such as manual searches and canine teams when the explosive detection or explosive trace detection systems are unavailable.

The passenger and checked baggage screening systems are composed of three elements: the people (TSOs) responsible for conducting the screening of airline passengers and their carry-on items and checked baggage, the technology used during the screening process, and the procedures TSOs are to follow to conduct screening. Collectively, these elements help to determine the effectiveness and efficiency of passenger and checked baggage screening operations.

Air Cargo Security

Air cargo ranges in size from one pound to several tons, and in type from perishables to machinery, and can include items such as electronic equipment, automobile parts, clothing, medical supplies, other dry goods, fresh cut flowers, fresh seafood, fresh produce, tropical fish, and human remains. Cargo can be shipped in various forms, including large containers known as unit loading devices that allow many packages to be consolidated into one container that can be loaded onto an aircraft, wooden crates, assembled pallets, or individually wrapped/boxed pieces, known as break bulk cargo.

Participants in the air cargo shipping process include shippers, such as individuals and manufacturers; indirect air carriers, also referred to as freight forwarders or regulated agents; air cargo handling agents, who process and load cargo onto aircraft on behalf of air carriers; and passenger and all-cargo carriers that store, load, and transport air cargo. A shipper may take its packages to a freight forwarder, or regulated agent, which consolidates cargo from many shippers and delivers it to air

⁶Explosive detection systems use computer-aided tomography X-rays to examine objects inside baggage and identify the characteristic signatures of threat explosives. This equipment operates in an automated mode.

⁷Explosive trace detection works by detecting vapors and residues of explosives. Human operators collect samples by rubbing bags with swabs, which are chemically analyzed to identify any traces of explosive materials.

carriers. A shipper may also send freight by directly packaging and delivering it to an air carrier's ticket counter or sorting center where either the air carrier or a cargo handling agent will sort and load cargo onto the aircraft. The shipper may also have cargo picked up and delivered by an all-cargo carrier, or choose to take cargo directly to a carriers' retail facility for delivery.

TSA's responsibilities for securing air cargo include, among other things, establishing security rules and regulations governing domestic and foreign passenger air carriers that transport cargo, domestic and foreign all-cargo carriers that transport cargo, and domestic indirect air carriers. TSA is also responsible for overseeing the implementation of air cargo security requirements by air carriers and indirect air carriers through compliance inspections, and, in coordination with DHS's S&T Director, for conducting research and development of air cargo security technologies. Air carriers (passenger and all-cargo) are responsible for implementing TSA security requirements, predominantly through a TSA-approved security program that describes the security policies, procedures, and systems the air carrier will implement and maintain in order to comply with TSA security requirements. Air carriers must also abide by security requirements issued by TSA through security directives or emergency amendments to air carrier security programs.

Air carriers use several methods and technologies to screen domestic and inbound air cargo.⁸ These include manual physical searches and comparisons between airway bills and cargo contents to ensure that the contents of the cargo shipment matches the cargo identified in documents filed by the shipper, as well as using approved technology, such as X-ray systems, explosive trace detection systems, decompression chambers, explosive detection systems, and certified explosive detection canine

⁸The Implementing Recommendations of the 9/11 Commission Act of 2007 defines the term 'screening' for purposes of air cargo to mean a physical examination or non-intrusive methods of assessing whether cargo poses a threat to transportation security. See 49 U.S.C. § 44901(g)(5). Such methods of screening include x-ray systems, explosives detection systems, explosives trace detection, explosives detection canine teams certified by TSA, or a physical search together with manifest verification. While additional methods may be approved to ensure that cargo does not pose a threat to transportation security, these additional methods cannot include solely performing a review of information about the contents of cargo or verifying the identity of a shipper of the cargo if not performed in conjunction with other authorized security methods, including whether a shipper is registered in the known shipper database.

teams.⁹ Under TSA's security requirements for domestic and inbound air cargo, passenger air carriers are currently required to randomly screen a specific percentage of non exempt air cargo pieces listed on each airway bill. All-cargo carriers are required to screen 100 percent of air cargo that exceeds a specific weight threshold. As of October 2006, domestic indirect air carriers are also required, under certain conditions, to screen a certain percentage of air cargo prior to its consolidation. TSA, however, does not regulate foreign freight forwarders, or individuals or businesses that have their cargo shipped by air to the United States. Under the Implementing Recommendations of the 9/11 Commission Act of 2007, DHS is required to implement a system to screen 50 percent of air cargo transported on passenger aircraft by February 2009, and 100 percent of such cargo by August 2010.¹⁰

Passenger Watch-List Matching

The prescreening of airline passengers who may pose a security risk before they board an aircraft is one of many layers of security intended to strengthen commercial aviation. One component of prescreening is passenger watch-list matching—or the process of matching passenger information against the No-Fly and Selectee lists to identify passengers who should be denied boarding or who should undergo additional security scrutiny.¹¹

Aircraft operators are currently responsible for checking passenger information against the No-Fly and Selectee lists to identify passengers who should be denied boarding or who should undergo additional security scrutiny. To further enhance commercial aviation security and in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), TSA is developing a program to assume from air carriers the function of matching passenger information against government-supplied

⁹ Certified explosive detection canine teams have been evaluated by TSA and shown to effectively detect explosive devices. Decompression chambers simulate the pressures acting on aircraft by simulating flight conditions, which cause explosives that are attached to barometric fuses to detonate.

¹⁰ See Pub. L. No. 110-53, § 1602(a), 121 Stat. 266, 477-480 (2007) (codified at 49 U.S.C. § 44901(g)).

¹¹ The No Fly and Selectee lists contain the names of individuals with known or suspected links to terrorism. These lists are subsets of the consolidated terrorist watch-list that is maintained by the Federal Bureau of Investigation's Terrorist Screening Center.

terrorist watch-lists for domestic flights.¹² Secure Flight is the program through which TSA plans to meet this requirement. Following domestic implementation, TSA, through Secure Flight, plans to assume responsibility from CBP for watch-list matching of passengers on international flights bound to and from the United States. Secure Flight's mission is to enhance the security of commercial air travel by:

- eliminating inconsistencies in current air carrier watch-list matching procedures,
- reducing the number of individuals who are misidentified as being on the No Fly or Selectee list,
- reducing the risk of unauthorized disclosure of sensitive watch-list information, and
- integrating the redress process so that individuals are less likely to be improperly or unfairly delayed or prohibited from boarding an aircraft.

TSA plans to implement Secure Flight in three releases. During Release One, which is currently ongoing and is scheduled to be completed in March 2008, TSA is developing and testing the Secure Flight system. During Release Two, scheduled to be conducted from April 2008 through August 2008, TSA plans to begin parallel testing with air carriers during which both Secure Flight and air carriers will perform watch-list matching. Finally, during Release Three, TSA is to develop the capability for "airline cutovers" during which Secure Flight plans to begin conducting all watch-list matching for domestic air passengers. Release Three is scheduled to begin in September 2008. After Release Three, domestic cutovers are expected to begin in January 2009 and be completed in July 2009. TSA plans to assume from CBP watch-list matching for flights departing from and to the United States some time after domestic cutovers are completed.

Over the last 4 years, we have reported that the Secure Flight program (and its predecessor CAPPS II) had not met key milestones or finalized its goals, objectives, and requirements, and faced significant development and

¹²See 49 U.S.C. § 44903(j)(2)(C).

implementation challenges.¹³ Acknowledging the challenges it faced with the program, TSA suspended the development of Secure Flight and initiated a reassessment, or re-baselining, of the program in February 2006, which was completed in January 2007. Since our last testimony on Secure Flight in February 2007, we were mandated by the Implementing Recommendations of the 9/11 Commission Act of 2007 to assess various aspects of Secure Flight's development and implementation.¹⁴ In accordance with the act, we reviewed (1) TSA's efforts to develop reliable cost and schedule estimates for Secure Flight; (2) progress made by TSA in developing and implementing the Secure Flight system, including the implementation of security controls; (3) TSA's efforts to coordinate with CBP to integrate Secure Flight with CBP's watch-list matching function for international flights; (4) TSA's plans to protect private passenger information under Secure Flight; and (5) DHS's efforts to assess the effectiveness of the current redress process for passengers misidentified as being on or wrongly assigned to the No Fly or Selectee list.¹⁵

TSA's available funding for the Secure Flight program during fiscal year 2007 was \$32.5 million.¹⁶ In fiscal year 2008, TSA received \$50 million along with statutory authority to transfer up to \$24 million to the program, making as much as \$74 million available for the program in fiscal year 2008, if necessary.¹⁷ For fiscal year 2009, TSA has requested \$82 million in funding to allow the agency to continue development and implementation of the Secure Flight program and the full assumption of the watch-list matching function in fiscal year 2010.

¹³ GAO, *Aviation Security: Progress Made in Systematic Planning to Guide Key Investment Decisions, but More Work Remains*, GAO-07-448T (Washington, D.C.: February 13, 2007).

¹⁴ See Pub. L. No. 110-53, § 1605(b), 121 Stat. 266, at 481-82.

¹⁵ GAO is also mandated to review DHS's certification of 10 conditions outlined in section 522(a) of the DHS Appropriations Act, 2005, related to the development and implementation of the Secure Flight program. See Pub. L. No. 110-161, § 513, 121 Stat. 1844 (2007).

¹⁶ Fifteen million was appropriated during fiscal year 2007 and \$17.5 million was carried over from the prior fiscal year, for a total of \$32.5 million.

¹⁷ See Pub. L. No. 110-161, § 550, 121 Stat. 1844.

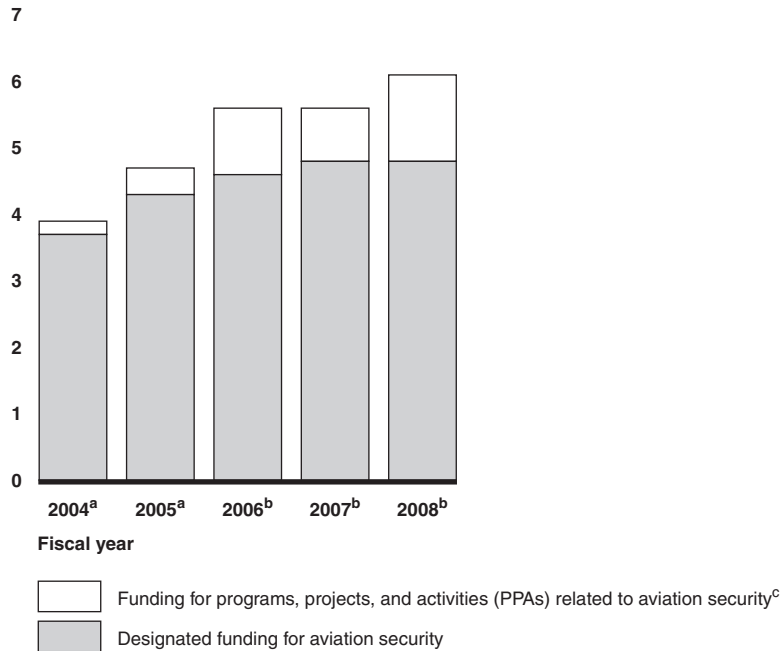
Aviation Security Fiscal Years 2004 through 2008 Funding and Fiscal Year 2009 Budget Request

According to DHS's budget execution reports and TSA's congressional budget justifications, TSA received appropriations for aviation security that total about \$26 billion since fiscal year 2004.¹⁸ During fiscal year 2004—the first year for which data were available—TSA received about \$3.9 billion for aviation security programs, and during fiscal year 2008, received about \$6.1 billion. The President's budget request for fiscal year 2009 includes about \$6.0 billion to continue TSA's aviation security activities. This total includes about \$5.3 billion specifically designated for aviation security and about \$0.76 billion for aviation-security related programs, such as Secure Flight, and mandatory fee accounts, such as the Aviation Security Capital Fund. Figure 1 identifies reported aviation security funding for fiscal years 2004 through 2008.

¹⁸DHS's budget execution reports are monthly statements that reflect the department's financial activity. In our analysis of DHS's budget execution reports and TSA Congressional Budget Justification, we included funding that we determined to be specifically designated for aviation security and funding for all programs, projects, and activities related to aviation security, to the extent they were identifiable, in order to present consistent total funding amounts across fiscal years. In addition, these aviation security totals do not reflect funding for activities that may support TSA's aviation security programs and projects, such as intelligence and administration, because DHS's documentation does not identify the proportion of funding dedicated to support aviation security. During this time period, a number of aviation security related activities were transferred in or out of TSA's jurisdiction, which affects TSA funding levels for the affected fiscal years.

Figure 1: TSA's Reported Aviation Security Funding for Fiscal Years 2004 through 2008

TSA's aviation security funding as reported by TSA (dollars in billions)



Source: GAO analysis of TSA budget execution reports for fiscal years 2004 to 2007 and TSA's Congressional Budget Justification for fiscal year 2009.

Note: We used the September 30th budget execution reports for our analysis of TSA funding for fiscal years 2004 through 2006. For fiscal years 2007 and 2008, we used TSA's fiscal year 2009 congressional budget justification. According to the budget execution reports and congressional budget justification, figures presented include all rescissions and supplemental funding for the fiscal years.

^aFiscal years 2004 and 2005 include approximately \$330 million in research and development funding for aviation security. Beginning in fiscal year 2006, research and development funding was consolidated within DHS S&T. Therefore, this funding, as reflected in TSA's budget documentation, is not included as part of TSA's appropriation from fiscal year 2006 forward.

^bFiscal years 2006, 2007, and 2008 include approximately \$680 million, \$720 million, and \$770 million respectively, in funding for the Federal Air Marshals Service, which was transferred back to TSA from U.S. Immigration and Customs Enforcement in October 2005. Federal Air Marshal Service funding is included within totals for related aviation security programs, projects, and activities for fiscal years 2006, 2007, and 2008.

^cFunding for aviation security-related programs, projects, and activities is reported separately. However, TSA designated funds from other programs, projects, and activities to aviation security as well, which represents the unshaded areas.

TSA Has Made Significant Enhancements to Its Passenger Screening Operations, but Can Further Strengthen Its Efforts

TSA has taken significant steps to strengthen the three key elements of the screening system—people (TSOs and private screeners), screening procedures, and technology—but has faced management, planning, and funding challenges. For example, TSA developed a Staffing Allocation Model to determine TSO staffing levels at airports that reflect current operating conditions, and implemented several initiatives intended to enhance the detection of threat objects, particularly improvised explosives. We reported that TSA also proposed modifications to passenger checkpoint screening procedures based on risk (threat and vulnerability information), among other factors, but, as we previously reported, could do more evaluation of proposed procedures before they are implemented to help ensure that they achieve their intended results. Finally, TSA is exploring new technologies to enhance the detection of explosives and other threats, but continues to face management and funding challenges in developing and fielding technologies at airport checkpoints.

Of the approximately \$6.0 billion requested for aviation security in the President's fiscal year 2009 budget request, about \$4.0 billion, or approximately 66 percent, is for passenger and checked baggage screening. This includes approximately \$3.9 billion to support passenger and checked baggage screening operations, such as TSO salaries and training, and about \$154 million for the procurement and installation of checked baggage explosive detection systems.¹⁹

TSA Has Efforts Under Way to Strengthen the Allocation of Its TSO Workforce

TSA has implemented several efforts intended to strengthen the allocation of its TSO workforce. We reported in February 2004 that staffing shortages and TSA's hiring process had hindered the ability of some Federal Security Directors (FSD)—the ranking TSA authorities responsible for leading and coordinating security activities at airports—to provide sufficient resources to staff screening checkpoints and oversee screening operations at their checkpoints without using additional measures such as overtime.²⁰ Since

¹⁹ According to TSA's Congressional Justification, the \$154 million requested for procurement and installation of checked baggage explosive detection systems is in addition to the \$676 in mandatory fees requested for the Aviation Security Capital Fund, which would provide \$830 million in total funding for the procurement and installation of such systems.

²⁰ GAO, *Aviation Security: Challenges Exist in Stabilizing and Enhancing Passenger and Baggage Screening Operations*, GAO-04-440T (Washington, D.C.: Feb. 12, 2004).

that time, TSA has developed a Staffing Allocation Model to determine TSO staffing levels at airports.²¹ In determining staffing allocations, the model takes into account the workload demands unique to each airport based on an estimate of each airport's peak passenger volume. This input is then processed against certain TSA assumptions about screening passengers and checked baggage—including expected processing rates, required staffing for passenger lanes and baggage equipment based on standard operating procedures, and historical equipment alarm rates. In August 2005, TSA determined that the Staffing Allocation Model contained complete and accurate information on each airport from which to estimate staffing needs, and the agency used the model to identify TSO allocations for each airport. At that time, the staffing model identified a total TSO full-time equivalent allocation need of 42,303 TSOs.

In addition to the staffing levels identified by the model, TSA sets aside TSO full-time equivalents for needs outside of those considered by the model in its annual allocation run for airports. For example, during the course of the year, certain airports may experience significant changes to their screening operations, such as the arrival of a new airline or opening of a new terminal. According to TSA officials, the agency established a reserve of 413 TSO full-time equivalents during fiscal year 2007 that can be used to augment the existing force, and began fiscal year 2008 with a reserve of 170 TSO full-time equivalents. TSA plans to continue with its use of a reserve force during fiscal year 2009 due to the dynamic nature of airport operations and the need to make staffing adjustments to meet changing operational requirements. Additionally, in order to handle short-term extraordinary needs at airports, TSA established a National Deployment Force—formerly known as the National Screening Force—comprised of TSOs and other TSA security staff who can be sent to airports to augment local TSO staff during periods of unusually high passenger volume, such as the Super Bowl. According to TSA, as of February 13, 2008, there were 451 TSOs in the National Deployment Force. The TSA fiscal year 2009 budget justification request identifies that TSA analyzes each request for support from the National Deployment Force from a cost, benefit, and risk perspective to ensure the optimal use of

²¹ As part of TSA's Screening Partnership Program, 10 airports and 1 heliport use private contract screeners in lieu of federal TSOs. Although these airports and heliport do not use federal screeners, TSA uses the Staffing Allocation Model to determine the full-time equivalent screening staff at each of these airports. These staffing levels, as determined by the model, serve as a limit on the number of private screeners that the private screening contractors could employ.

resources. The budget justification requests \$34.3 million for operational expenses for the National Deployment Office—the office responsible for, among other things, deploying the National Deployment Force to those airports experiencing significant staffing shortfalls.

FSDs we interviewed during 2006 as part of our review of TSA's staffing model generally reported that the model is a more accurate predictor of staffing needs than TSA's prior staffing model, which took into account fewer factors that affect screening operations. However, FSDs identified that some assumptions used in the fiscal year 2006 staffing model did not reflect actual operating conditions. For example, FSDs noted that the staffing model's assumption of a 20 percent part-time workforce—measured in terms of full-time equivalents—had been difficult to achieve, particularly at larger (category X and I) airports, because of, among other things, economic conditions leading to competition for part-time workers, remote airport locations coupled with a lack of mass transit, TSO base pay that had not changed since fiscal year 2002, and part-time workers' desire to convert to full-time status. We reported in February 2007 that TSA data showed that for fiscal years 2005 and 2006, the nation's category X airports had a TSO workforce composed of about 9 percent part-time equivalents, and the part-time TSO attrition rate nationwide remained considerably higher than the rate for full-time personnel (approximately 46 percent versus 16 percent for full-time TSOs during fiscal year 2006).²² According to TSA's fiscal year 2009 congressional budget justification, full-time TSO attrition nationwide decreased to 11.6 percent during 2007, and part-time attrition decreased to 37.2 percent. FSDs also expressed concern that the model did not specifically account for the recurrent training requirement for TSOs of 3 hours per week averaged over a fiscal year quarter. FSDs further identified that the model for fiscal year 2006 did not account for TSO's time away from screening to perform operational support duties, such as payroll processing, scheduling, distribution and maintenance of uniforms, data entry, and workman's compensation processing. To help ensure that TSOs are effectively utilized, we recommended that TSA establish a policy for when TSOs can be used to provide operational support. Consistent with our recommendation, in March 2007, TSA issued a management directive that provides guidance on assigning TSOs, through detail or permanent promotion, to duties of another position for a specified period of time.

²² GAO, *Aviation Security: TSA's Staffing Allocation Model Is Useful for Allocating Staff among Airports, but Its Assumptions Should Be Systematically Reassessed*, GAO-07-299 (Washington, D.C.: February 28, 2007).

In response to FSDs' input and the various mechanisms TSA had implemented to monitor the sufficiency of the model's allocation outputs, TSA made changes to some assumptions in the model for fiscal year 2007. For example, TSA recognized that some airports cannot likely achieve a 20 percent part-time equivalent level and others, most likely smaller airports, may operate more efficiently with other levels of part-time TSO staff. As a result, for fiscal year 2007, TSA modified the assumption in its Staffing Allocation Model to include a variable part-time goal based on each airport's historic part-time to full-time TSO ratio. TSA also included an allowance in the model for fiscal 2007 to provide additional assurance that TSOs complete required training on detecting improvised explosive devices, as well as an allowance for operational support duties to account for the current need for TSOs to perform these duties. In our February 2007 report on the Staffing Allocation Model, we recommended that TSA establish a formal, documented plan for reviewing all of the model assumptions on a periodic basis to ensure that the assumptions result in TSO staffing allocations that accurately reflect operating conditions that may change over time. TSA agreed with our recommendation and, in December 2007, developed a Staffing Allocation Model Rates and Assumptions Validation Plan. The plan identifies the process TSA will use to review and validate the model's assumptions on a periodic basis.

Although we did not independently review TSA's staffing allocation for fiscal year 2008, the TSA fiscal year 2009 budget justification identified that the agency has achieved operational and efficiency gains that enabled them to implement or expand several workforce initiatives involving TSOs, which are summarized in table 2. For example, TSA reported making several changes to the fiscal year 2008 Staffing Allocation Model, such as decreasing the allocation for time paid not worked (annual, sick, and military leave; compensatory time; and injury time off) from a 14.5 percent to 14 percent based on past performance data. TSA also reported revising the exit lane staffing based on each checkpoint's unique operating hours rather than staffing all exit lanes based on the maximum open hours for any checkpoint at an airport.

Table 2: TSA Workforce Initiatives Involving Transportation Security Officers (TSOs)

Workforce initiative	Description of initiative
Travel document checker	TSA implemented the travel document checker initiative at over 250 smaller airports during fiscal year 2007. According to the TSA fiscal year 2009 budget justification, through savings realized through adjustments in the fiscal year 2008 Staffing Allocation Model, TSA was able to fund 1,033 additional full-time-equivalent TSOs for the travel document checker initiative. This program is intended to ensure that only passengers with authentic travel documents access the sterile areas of airports and board aircraft. TSA's budget justification identifies that in fiscal year 2007 the agency implemented this program at over 340 of the 450 airports with federal TSOs.
Behavior detection officers	TSA completed its planned deployment of the behavior detection officer program. These officers screen passengers by observation technique (also known as SPOT) to identify potentially high-risk passengers based on involuntary physical and physiological reactions. During fiscal year 2007, 643 behavior detection officers were deployed at 42 airports.
Bomb appraisal officers	TSA completed the planned deployment of the Bomb Appraisal Officer program. These officers, who have undergone training in the disposal of explosives, provide formal training to TSOs to increase their ability to recognize potential improvised explosive devices and components. The Bomb Appraisal Officer Program was formally implemented at 107 airports during fiscal year 2007.
Visible Intermodal Protection and Response Teams	According to TSA, the agency deployed Visible Intermodal Protection and Response Teams to airports around the country. These teams—comprised of TSOs, behavior detection officers and other aviation security employees—are responsible for screening passengers, looking for suspicious behavior, and acting as a visible deterrent in multiple transportation sectors, including buses, mass transit stations, and airports. TSA's budget justification identified that as of February 2008, TSA had deployed over 100 Visible Intermodal Protection and Response Teams to airports and mass transit systems around the country.
Aviation Direct Access Screening Program	The Aviation Direct Access Screening Program is intended to provide uniform procedures and standards for TSOs to screen individuals, their accessible property, and vehicles upon entering secure airport areas, and conduct visual inspections of aircraft. Under this program, TSOs are to screen aviation workers and inspect for the presence of explosives, incendiaries, weapons, and other prohibited items, improper airport identification media, and items identified through specific intelligence. In March 2007, TSA required Federal Security Directors to implement the Aviation Direct Screening Program at each of their assigned airports.

Source: TSA Fiscal Year 2009 budget justification.

TSA's fiscal year 2009 budget justification includes \$2.7 billion for the federal TSO workforce represents an increase of about \$80 million over fiscal year 2008. Of the \$80 million increase, about \$38 million is for cost of living adjustments, and about \$42 million is for the annualization of the full-year cost of the Behavior Detection Officer and Aviation Direct Access Screening Program positions. According to the budget justification, the \$2.7 billion includes funding for compensation and benefits of 45,643 full-

time equivalent personnel—approximately 46,909 TSOs and about 1,100 screening managers.²³ Table 3 identifies the total TSO and screening manager full-time equivalents and the funding levels for fiscal years 2005 through 2008, as reported by TSA.

Table 3: Passenger and Checked Baggage TSO and Screening Manager Full-time Equivalents and Actual Spending for TSO Personnel, Compensation, and Benefits, by Fiscal Year

Fiscal year	FY 2005	FY 2006	FY 2007	FY 2008 ^a
Total TSOs and screening managers at airports nationwide	45,690	42,187	42,592	45,438
Actual spending (dollars in thousands)	\$2,291,572	\$2,251,503	\$2,444,455	\$2,636,104

Source: TSA.

^aFiscal year 2008 figures represent TSA's budget in accordance with funds appropriated through Division E of the Consolidated Appropriations Act, 2008.

TSA Has Taken Steps to Strengthen Passenger Screening Procedures, but Could Improve Its Evaluation and Documentation of Proposed Procedures

In addition to TSA's efforts to deploy a federal TSO workforce, TSA has taken steps to strengthen passenger checkpoint screening procedures to enhance the detection of prohibited items. However, we have identified areas where TSA could improve its evaluation and documentation of proposed procedures. In April 2007, we reported that TSA officials considered modifications to its standard operating procedure (SOP) based on risk information (threat and vulnerability information), daily experiences of staff working at airports, and complaints and concerns raised by the traveling public.²⁴ In addition to these factors, consistent with its mission, TSA senior leadership made efforts to balance the impact that proposed SOP modifications would have on security, efficiency, and customer service when deciding whether proposed SOP modifications should be implemented. For example, in August 2006, TSA sought to increase security by banning liquids and gels from being carried onboard aircraft in response to the alleged terrorist plot to detonate liquid explosives onboard multiple aircraft en route from the United Kingdom to

²³The TSA fiscal year 2009 budget justification includes about \$151 million for the Screening Partnership Program.

²⁴ GAO, *Aviation Security: Risk, Experience, and Customer Concerns Drive Changes to Airline Passenger Screening Procedures, but Evaluation and Documentation of Proposed Changes Could Be Improved*, GAO-07-634 (Washington, D.C.: April 16, 2007).

the United States. In September 2006, after obtaining more information about the alleged terrorist plot—to include information from the United Kingdom and U.S. intelligence communities, discussions with explosives experts, and testing of explosives—TSA officials decided to lift the total ban on liquids and gels to allow passengers to carry small amounts of liquids and gels onboard aircraft. TSA officials also lifted the total ban because banning liquids and gels as carry-on items was shown to affect both efficiency and customer service. In an effort to harmonize its liquid screening procedures with other countries, in November 2006, TSA revised its procedures to allow 3.4 fluid ounces of liquids, gels, and aerosols onboard aircraft.

We further reported that for more significant SOP modifications, TSA first tested the proposed modifications at selected airports to help determine whether the changes would achieve their intended purpose, as well as to assess its impact on screening operations. TSA's efforts to collect quantitative data through testing proposed procedures prior to deciding whether to implement or reject them is consistent with our past work that has shown the importance of data collection and analyses to support agency decision making. However, we reported that TSA's data collection and analyses could be improved to help TSA determine whether proposed procedures that are operationally tested would achieve their intended purpose. Specifically, we found that for tests of proposed screening procedures TSA conducted from April 2005 through December 2005, including the removal of small scissors and small tools from the prohibited items list, although TSA collected some data on the efficiency of and customer response to the procedures at selected airports, the agency generally did not collect the type of data or conduct the necessary analysis that would yield information on whether the proposed procedures would achieve their intended purpose. We also found that TSA's documentation on proposed modifications to screening procedures was not complete. We recommended that TSA develop sound evaluation methods, when possible, to assess whether proposed screening changes would achieve their intended purpose and generate and maintain documentation on proposed screening changes that are deemed significant. DHS generally agreed with our recommendations and TSA has taken steps to implement them. For example, for several proposed SOP changes considered during the fall of 2007, TSA provided documentation that identified the sources of the proposed changes and the reasons why the agency decided to accept or reject the proposed changes. With regard to our recommendation to develop sound evaluation methods when assessing proposed SOP modifications, when possible, TSA reported that it is working with subject matter experts to ensure that the agency's operational tests related to

proposed changes to screening procedures are well designed and executed, and produce results that are scientifically valid and reliable. These actions, when fully implemented, should enable TSA to better justify its passenger screening procedure modifications to Congress and the traveling public.

Once proposed SOP changes have been implemented, it is important that TSA have a mechanism in place to ensure that TSOs are complying with established procedures. In our April 2007 report, we identified that TSA monitors TSO compliance with passenger checkpoint screening SOPs through its performance accountability and standards system and through local and national covert testing. According to TSA officials, the performance accountability and standards system was developed in response to a 2003 report by us that recommended that TSA establish a performance management system that makes meaningful distinctions in employee performance,²⁵ and in response to input from TSA airport staff on how to improve passenger and checked baggage screening measures. This system is used by TSA to assess agency personnel at all levels on various competencies, including, among other things, technical proficiency. During fiscal year 2007, the technical proficiency component of the performance accountability and standards system for TSOs focused on TSO knowledge of screening procedures; image recognition; proper screening techniques; and the ability to identify, detect, and locate prohibited items. In addition to implementing the performance accountability and standards system, TSA also conducts local and national covert tests to evaluate, in part, the extent to which TSOs' noncompliance with SOPs affects their ability to detect simulated threat items hidden in accessible property or concealed on a person. In our April 2007 report, we identified that some TSA airport officials have experienced resource challenges in implementing these compliance monitoring efforts. TSA headquarters officials stated that they were taking steps, such as automating the performance accountability and standards system data entry functions, to address this challenge. Since then, TSA has also implemented a new local covert testing program nationwide, known as the Aviation Screening Assessment Program. This program is intended to measure TSO performance using realistic and standardized test scenarios to achieve a national TSO assessment measurement. According to TSA's fiscal year 2009 congressional budget justification, this national baseline

²⁵GAO, Transportation Security Administration: *Actions and Plans to Build a Results Oriented Culture*, GAO-03-190 (Washington, D.C.: January 2003).

measurement will be achieved by conducting a total of 48,000 annual tests. TSA plans to use the test results to identify vulnerabilities across screening operations and to provide recommendations for addressing the vulnerabilities to various stakeholders within TSA.

DHS and TSA Are Pursuing New Checkpoint Technologies to Enhance the Detection of Explosives and Other Threats, but Continue to Face Challenges

We reported in February 2007²⁶ that DHS S&T and TSA²⁷ were exploring new passenger checkpoint screening technologies to enhance the detection of explosives and other threats. However, we found that limited progress had been made in fielding explosives detection technology at passenger screening checkpoints, in part due to challenges DHS S&T and TSA faced in coordinating research and development efforts. TSA requested \$103.2 million in its fiscal year 2009 budget request for checkpoint technology and checkpoint reconfiguration. Specifically, the request includes \$91.7 million to, among other things, procure and deploy Advanced Technology Systems to further extend explosives and prohibited item detection coverage at category X and I checkpoints. The budget request identifies that equipment purchases may also include the Whole Body Imager, Bottled Liquids Scanner, Cast and Prosthesis Imager, shoe scanner systems, technology integration solutions, and additional units or upgrades to legacy equipment, and other technologies. TSA further requested \$11.5 million to support the optimization and reconfiguration of additional checkpoint lanes to accommodate anticipated airport growth and maintain throughput at the busiest airport checkpoints.

Of the various emerging checkpoint screening projects funded by TSA and DHS S&T, the explosive trace portal and the bottled liquids scanning device have been deployed to airport checkpoints, and a number of additional projects have initiated procurements or are being researched

²⁶ GAO, *Aviation Security: Progress Made in Systematic Planning to Guide Key Investment Decisions, but More Work Remains*, GAO-07-448T (Washington, D.C.: February 13, 2007).

²⁷ DHS S&T is responsible for research and development of checkpoint technologies related to aviation security, managing the activities conducted at the Transportation Security Laboratory, and coordinating these efforts with TSA. TSA's Passenger Screening Program is responsible for evaluating and deploying systems to detect explosives and weapons concealed on persons or in carry-on items, while strengthening access control, improving screener performance, and reducing staffing requirements.

and developed.²⁸ Projects which have initiated procurements include the cast and prosthesis scanner and advanced technology systems. Projects currently in research and development include the checkpoint explosives detection system and the whole body imager. Table 4 provides a description of passenger checkpoint screening technologies that have been deployed as well as technologies that have initiated procurements or are in research and development. This list of technologies is limited to those for which TSA could provide documentation. TSA is planning to develop and deploy additional technologies. We are continuing to assess TSA's deployment of new checkpoint screening technologies in our ongoing work and expect to report on the results of this work later this year.

²⁸Research and development projects generally fall within the following phases: (1) basic research includes all scientific efforts and experimentation directed to increase knowledge and understanding in the fields of science related to long-term national needs; (2) applied research includes efforts directed toward solving specific problems with a focus on developing and evaluating the feasibility of proposed solutions; (3) advanced development includes efforts directed toward the development of hardware for field experiments; and (4) operational testing includes evaluation of technologies in a realistic operating environment to assess the performance or cost reduction potential of advanced technology.

Table 4: Description of Passenger Checkpoint Screening Technologies Deployed, Procured, or in Research and Development as of January 2008

Technology	Description	Status
Explosives trace portals	Detects trace amounts of explosives on persons (will reduce the size of the current explosives trace portals at checkpoints).	TSA initiated deployment of 95 portals to airports. However, in June 2006, TSA halted the acquisition and deployment of the portals due to performance and maintenance issues. Currently, 114 portals are in storage, which were purchased at a total cost of over \$20 million.
Bottled liquids scanners	Screens for liquid explosives.	During fiscal year 2007, TSA procured 200 units. One-hundred and forty three units have been deployed to airports. For fiscal year 2008, TSA plans to procure 700 units.
Cast and prosthesis scanners	Provides a 2-dimensional image of the area beneath a cast or inside a prosthetic device.	TSA procured 34 units during fiscal year 2007 and expects delivery of the first unit in February 2008. TSA plans to deploy this technology to airports during 2008.
Advanced Technology Systems	TSA plans to replace the Threat Image Projection Ready X-ray machines currently used at category X airports with Advanced Technology Systems that are intended to improve detection capability and performance.	During 2007, testing was conducted on this technology, including operational testing at four airports. TSA procured 250 units during fiscal year 2007, and plans to procure 677 units and deploy 429 units during fiscal year 2008.
Checkpoint explosives detection systems	Creates a three dimensional image of bags to detect explosives and other nonmetallic items.	This technology is currently undergoing various types of testing, including operational testing. During fiscal year 2007, TSA procured 20 units to be deployed starting in 2008.
Whole body imagers	Provides two-dimensional, full-body images of all items on a passenger's body, including plastic explosives and concealed metallic, non-metallic, and ceramic or plastic objects.	TSA is conducting operational pilot testing of the whole body imager at three airports. If the testing is successful, TSA plans to procure and deploy the first units to airports during 2008.

Source: TSA.

Despite TSA's efforts to develop passenger checkpoint screening technologies, we reported that limited progress has been made in fielding explosives detection technology at airport checkpoints. For example, we reported that TSA had anticipated that the explosives trace portals would be in operation throughout the country during fiscal year 2007. However, due to performance and maintenance issues, TSA halted the acquisition and deployment of the portals in June 2006. As a result, TSA has fielded less than 25 percent of the 434 portals it projected it would deploy by fiscal year 2007. TSA officials are considering what to do with the portals that were procured and are currently in storage. In addition to the portals,

TSA has fallen behind in its projected acquisition of other emerging screening technologies. For example, we reported that the acquisition of 91 Whole Body Imagers was previously delayed in part because TSA needed to develop a means to protect the privacy of passengers screened by this technology. TSA also reduced the initial number of the cast and prosthesis scanner units to be procured during fiscal year 2007 due to unexpected maintenance cost increases. Furthermore, fiscal year 2008 funding to procure additional cast and prosthesis scanners was shifted to procure more Whole Body Imagers and Advanced Technology Systems due to a change in priorities.

While TSA and DHS have taken steps to coordinate the research, development, and deployment of checkpoint technologies, we reported in February 2007 that challenges remained. For example, TSA and DHS S&T officials stated that they encountered difficulties in coordinating research and development efforts due to reorganizations within TSA and S&T. A senior TSA official further stated at the time that, while TSA and the DHS S&T have executed a memorandum of understanding to establish the services that the Transportation Security Laboratory is to provide to TSA, coordination with S&T remained a challenge because the organizations had not fully implemented the terms of the agreement. Since our February 2007 testimony, according to TSA and S&T, coordination between them has improved.

We also reported that TSA did not have a strategic plan to guide its efforts to acquire and deploy screening technologies, and that a lack of a strategic plan or approach could limit TSA's ability to deploy emerging technologies at those airport locations deemed at highest risk. The Consolidated Appropriations Act, 2008, provides that, of TSA's appropriated funds for Transportation Security Support, \$10,000,000 may not be obligated until the Secretary of Homeland Security submits to the House and Senate Committees on Appropriations detailed expenditure plans for checkpoint support and explosive detection systems refurbishment, procurement, and installation on an airport-by-airport basis for fiscal year 2008, along with the strategic plan for checkpoint technologies previously requested by the committees. The Act further requires that the expenditure and strategic plans be submitted no later than 60 days after the date of enactment of the Act (enacted December 26, 2007). According to TSA officials, they currently plan to submit the strategic plan to Congress by June 2008. We will continue to evaluate DHS S&T's and TSA's efforts to research, develop and deploy checkpoint screening technologies as part of our ongoing review.

TSA Has Taken Action to Strengthen Air Cargo Security, but Additional Efforts Are Needed

TSA has taken steps to enhance domestic and inbound air cargo security, but more work remains to strengthen this area of aviation security. For example, TSA has issued an Air Cargo Strategic Plan that focused on securing the domestic air cargo supply chain. However, in April 2007, we reported that this plan did not include goals and objectives for addressing the security of air cargo transported into the United States from another country, which presents different security challenges than cargo transported domestically.²⁹ We also reported that TSA had not conducted vulnerability assessments to identify the range of security weaknesses that could be exploited by terrorists related to air cargo operations, and recommended that TSA develop a methodology and schedule for completing these assessments. In response, in part, to our recommendation, TSA implemented an Air Cargo Vulnerability Assessment program and plans to complete assessments of all Category X airports by 2009. In addition, we also reported that TSA had established requirements for air carriers to randomly screen air cargo, but had exempted some domestic and inbound cargo from screening. To address these exemptions, TSA issued a security directive and emergency amendment in October 2006 to domestic and foreign air carriers operating within and from the United States that limited the screening exemptions. Moreover, based on our recommendation to systematically analyze compliance inspection results and use the results to target future inspections, TSA recently reported that the agency has increased the number of inspectors dedicated to conducting domestic air cargo compliance inspections, and has begun analyzing the results of these inspections to prioritize their inspections on those entities that have the highest rates of noncompliance, as well as newly approved entities that have yet to be inspected. With respect to inbound air cargo, we reported that TSA lacked an inspection plan with performance goals and measures for its inspection efforts, and recommended that TSA develop such a plan. In response to our recommendation, TSA officials stated that the agency formed an International Cargo Working Group to develop inspection prompts to guide inspectors in their examinations of foreign and U.S. air cargo operators departing from foreign locations to the United States. In addition to taking steps to strengthen inspections of air cargo, TSA is working to enhance air cargo screening technologies. Specifically, we reported in October 2005 and again in April 2007 that TSA, working with DHS's S&T, was developing and pilot testing a number of technologies to

²⁹ GAO, *Aviation Security: Federal Efforts to Secure U.S.-Bound Air Cargo Are in the Early Stages and Could Be Strengthened*, GAO-07-660 (Washington, D.C.: April 2007).

assess their applicability to screening and securing air cargo. According to TSA officials, the agency will determine whether it will require the use of any of these technologies once it has completed its assessments and analyzed the results. Finally, TSA is taking steps to compile and analyze information on air cargo security practices used abroad to identify those that may strengthen DHS's overall air cargo security program, as we recommended. According to TSA officials, the design of the Certified Cargo Screening Program is based on the agency's review of foreign countries' models for using government-certified shippers and freight forwarders to screen air cargo earlier in the supply chain. TSA officials believe that this program will assist the agency in meeting the requirement to screen 100 percent of air cargo transported on passenger aircraft by August 2010, as mandated by the Implementing Recommendations of the 9/11 Commission Act of 2007.³⁰ We have not independently reviewed the Certified Cargo Screening Program.

TSA's Air Cargo Strategic Plan and Vulnerability Assessments Can Be Strengthened

DHS has taken steps towards applying a risk-based management approach to addressing air cargo security, including conducting assessments of the threats posed to air cargo operations. However, we have reported that opportunities exist to strengthen these efforts. Applying a risk management framework to decision making is one tool to help provide assurance that programs designed to combat terrorism are properly prioritized and focused. As part of TSA's risk-based approach, TSA issued an Air Cargo Strategic Plan in November 2003 that focused on securing the domestic air cargo supply chain. However, in April 2007, we reported that this plan did not include goals and objectives for addressing inbound air cargo security, or cargo that is transported into the United States from another country, which presents different security challenges than cargo transported domestically.³¹ To ensure that a comprehensive strategy for securing inbound air cargo exists, we recommended that DHS develop a risk-based strategy to address inbound air cargo security that should define TSA's and CBP's responsibilities for ensuring the security of inbound air cargo. In response to our recommendation, CBP issued its International Air Cargo Security Strategic Plan in June 2007. While this plan identifies how CBP will partner with TSA, it does not specifically

³⁰ In fulfilling this mandate, DHS must provide for the screening of 50 percent of all cargo transported on passenger aircraft by February 2009, 18 months after enactment of the Act. See 49 U.S.C. § 44901(g).

³¹See GAO-07-660.

address TSA's responsibilities in securing inbound air cargo. According to TSA officials, the agency plans to revise its Air Cargo Strategic Plan during the third quarter of fiscal year 2008, and will incorporate a strategy for addressing inbound air cargo security, including how the agency will partner with CBP. TSA reported that the updated strategic plan will also incorporate the requirement that TSA develop a system to screen 100 percent of air cargo prior to its transport on passenger aircraft as required by the Implementing Recommendations of the 9/11 Commission Act of 2007.

In addition to developing a strategic plan, a risk management framework in the homeland security context should include risk assessments, which typically involve three key elements—threats, vulnerabilities, and criticality or consequence. Information from these three assessments provides input for setting priorities, evaluating alternatives, allocating resources, and monitoring security initiatives. In September 2005, TSA's Office of Intelligence completed an overall threat assessment for air cargo, which identified general and specific threats to both domestic and inbound air cargo. However, in October 2005, and again in April 2007, we reported that TSA had not conducted vulnerability assessments to identify the range of security weaknesses that could be exploited by terrorists related to air cargo operations, and recommended that TSA develop a methodology and schedule for completing these assessments.³² In response, in part, to our recommendation, TSA implemented an Air Cargo Vulnerability Assessment program in November 2006. TSA officials reported that to date, the agency has completed vulnerability assessments at six domestic airports and plans to complete vulnerability assessments at all domestic Category X airports by 2009. Officials further stated that the results of these assessments will assist the agency with its efforts to collaborate with foreign governments to conduct joint assessments at foreign airports that will include a review of air cargo vulnerabilities.

³² GAO, *Aviation Security: Federal Action Needed to Strengthen Domestic Air Cargo Security*, GAO-06-76 (Washington, D.C.: October 2005) and GAO-07-660.

TSA Is Working to Revise Inspection Exemptions, Enhance Its Compliance Inspection Activities, and Develop Technologies for Air Cargo

In October 2005 and April 2007, we also reported that TSA had established requirements for air carriers to randomly screen air cargo, but had exempted some domestic and inbound cargo from screening. We recommended that TSA examine the rationale for existing domestic and inbound air cargo screening exemptions and determine whether such exemptions left the air cargo system unacceptably vulnerable. TSA established a working group to examine the rationale for these exemptions, and in October 2006, issued a security directive and emergency amendment to domestic and foreign passenger air carriers operating within and from the United States that limited the screening exemptions.³³ The security directive and emergency amendment, however, did not apply to inbound air cargo. The Implementing Recommendations of the 9/11 Commission Act of 2007 requires DHS to conduct an assessment of screening exemptions granted under 49 U.S.C. § 44901(i)(1) for cargo transported on passenger aircraft and an analysis to assess the risk of maintaining such exemptions. According to TSA, the agency will propose a number of revisions to certain alternate means of screening for particular cargo types transported on passenger aircraft departing from both domestic and foreign locations in its assessment of current screening exemptions. Although this report was due to Congress by December 3, 2007, it has yet to be submitted.

We also reported that TSA conducted compliance inspections of air carriers to ensure that they are meeting existing air cargo security requirements. However, in October 2005, we found that TSA had not developed measures to assess the adequacy of air carrier compliance with air cargo security requirements, or assessed the results of its domestic compliance inspections to target higher-risk air carriers or indirect air carriers for future reviews. TSA has since reported that the agency has increased the number of inspectors dedicated to conducting domestic air cargo inspections, and has begun analyzing the results of the compliance inspections to prioritize their inspections on those entities that have the highest rates of noncompliance, as well as newly approved entities that have yet to be inspected. With respect to inbound air cargo, we reported in April 2007 that TSA lacked an inspection plan with performance goals and measures for its inspection efforts, and recommended that TSA

³³TSA also issued a security directive to passenger air carriers with flights operating from and/or within the United States in July 2007 further clarifying the air cargo screening exemptions. This security directive, however, did not apply to air carriers transporting cargo into the United States.

develop such a plan. In February 2008, TSA officials stated that the agency formed an International Cargo Working Group to develop inspection prompts to guide International Cargo Transportation Security Inspectors in their inspections of the various air cargo operations. According to TSA, using these prompts will allow the agency to evaluate both foreign and U.S. air cargo operators departing from foreign locations to the United States.

In addition to taking steps to strengthen inspections of air cargo, TSA is working to enhance air cargo screening technologies. Specifically, we reported in October 2005 and again in April 2007 that TSA, working with S&T, was developing and pilot testing a number of technologies to assess their applicability to screening and securing air cargo. These efforts included an air cargo explosives detection pilot program implemented at three airports; an EDS pilot program; an air cargo security seals pilot; the use of hardened unit-loading devices; and the use of pulsed fast neutron analysis.³⁴ According to TSA officials, the agency will determine whether it will require the use of any of these technologies once it has completed its assessments and analyzed the results. As of February 2008, TSA has provided timeframes for completing one of these assessments, the EDS cargo pilot program. DHS officials added that once the department has determined which technologies it will approve for use for domestic air cargo, they will consider the use of these technologies for enhancing the security of inbound air cargo shipments. According to TSA officials, the federal government and the air cargo industry face several challenges that must be overcome to effectively implement any of these technologies to screen or secure air cargo. These challenges include factors such as the nature, type, and size of cargo to be screened; environmental and climatic conditions that could impact the functionality of screening equipment; slow screening throughput rates; staffing and training issues for individuals who screen air cargo; the location of air cargo facilities; the

³⁴ Specifically, the air cargo explosives detection program, implemented at three airports, tested the use of explosive detection systems, explosive trace detectors, standard X-ray machines, canine teams, technologies that can locate a stowaway, and manual screening of air cargo. The EDS pilot program tested the use of computer-aided tomography to measure the densities of objectives in order to identify potential explosives in air cargo. Further, the air cargo security seals project is exploring the viability of potential security countermeasures, such as tamper-evident security seals. TSA is also testing the use of hardened unit-loading devices, which are containers made of blast-resistant material that could withstand an explosion onboard an aircraft. Finally, the use of pulsed fast neutron analysis, which allows for the identification of the material signatures of contraband, explosives, and other threat objects, is also being tested in the air cargo environment.

cost and availability of screening technologies; and employee health and safety concerns, such as worker exposure to radiation. According to TSA officials, there is no single technology capable of efficiently and effectively screening all types of air cargo for the full range of potential terrorist threats, including explosives and weapons of mass destruction.

TSA Has Taken Steps to Review Air Cargo Practices Used Abroad to Strengthen the Department's Overall Air Cargo Security Program

Our review of inbound air cargo security also identified some security practices that are currently not used by TSA but that could help strengthen the security of inbound and domestic air cargo supply chains. In April 2007, we recommended that TSA, in collaboration with foreign governments and the U.S. air cargo industry, systematically compile and analyze information on air cargo security practices used abroad to identify those that may strengthen the department's overall air cargo security program. TSA agreed with this recommendation and, since the issuance of our report, proposed a new program, the Certified Cargo Screening Program, to assist the agency in meeting the requirement to screen 100 percent of air cargo transported on passenger aircraft by August 2010, as mandated by the Implementing Recommendations of the 9/11 Commission Act of 2007. According to TSA officials, the agency reviewed the models used by two foreign countries to use government-certified screeners to screen air cargo earlier in the supply chain, when designing their Certified Cargo Screening Program. TSA officials stated that the intention of the Certified Cargo Screening Program is to allow large shippers and/or manufacturers, who are certified by TSA, referred to as TSA-Certified Cargo Screening Facilities, to screen air cargo before it leaves the factory. According to TSA officials, employees performing the screening at these certified facilities would need to undergo a security threat assessment, and be trained in screening and inspection procedures. The facilities would also have to purchase the necessary screening equipment. After screening, the cargo would be secured with a tamper resistant seal and transported to the airport for shipment. The air carriers will be responsible for ensuring that 100 percent of cargo that they accept for transport has been screened by the TSA-Certified Cargo Screening Facilities. In January 2008, TSA began phase one of its pilot testing at one airport and plans to expand this pilot program to five other airports within three months. According to TSA, as part of its plans to screen 100 percent of air cargo on passenger aircraft, the agency also plans to pilot test a proposed system for targeting specific domestic air cargo shipments, referred to as Freight Assessment. Specifically, the Freight Assessment System will identify elevated risk cargo at various points in the supply chain for additional scrutiny, which could include secondary screening. TSA, however, did not provide us with

information on the duration of the pilot test or when the Freight Assessment System would be fully operational.

For fiscal year 2009, the President's budget includes a request of about \$100 million for TSA's air cargo security program. Specifically, TSA is requesting \$51.9 million for 450 air cargo inspectors, \$26.5 million for 170 canine teams, and \$15.9 million for the Certified Cargo Screening Program.³⁵

TSA Has Made Progress in Developing and Implementing the Secure Flight Program, but Can Further Strengthen Its Efforts

TSA has made substantial progress in instilling more discipline and rigor into Secure Flight's development and implementation since we last reported on the program in February 2007, but challenges remain that may hinder the program's progress moving forward. TSA developed a detailed concept of operations, established a cost and schedule baseline, and drafted key management and systems development documents, among other systems development efforts. TSA also has plans to integrate DHS's domestic and international watch-list matching functions, and has strengthened efforts to protect passenger information, including publishing a proposed rulemaking for the Secure Flight Program and privacy notices that address key privacy protection principles, consistent with our past recommendations. However, despite these successes, TSA continues to face some program management challenges in developing the program. Specifically, while TSA developed a life-cycle cost estimate and an integrated master schedule for Secure Flight, the program has not fully followed best practices that would help to ensure reliable and valid cost and schedule estimates, and the program schedule has experienced slippages. We also found that TSA can strengthen its systems development efforts by demonstrating that it has fully implemented its risk management plan, incorporated end-to-end testing³⁶ as part of the program's testing strategy, and more fully addressed system security requirements and vulnerabilities. We also found that DHS and TSA can strengthen their assessment of the current redress process for passengers who believe they were inappropriately inconvenienced during the watch-list matching process. TSA officials stated that they have considerably strengthened Secure Flight's systems development efforts, and have already taken or plan to take action to address the issues we identified.

³⁵According to TSA, the funding requested for the Certified Cargo Screening Program could change if the agency has any contract activity in fiscal year 2008 for this program.

³⁶End-to-end testing is conducted to verify that the entire system, including any external systems with which it interfaces, functions as intended in an operational environment.

TSA Has Made Progress in Strengthening Secure Flight's Development and Implementation

TSA has taken numerous steps to address previous GAO recommendations related to strengthening Secure Flight's development and implementation, as well as additional steps designed to strengthen the program.³⁷ TSA has, among other things, developed a detailed, conceptual description of how the system is to operate, commonly referred to as a concept of operations; established a cost and schedule baseline; developed security requirements; developed test plans; conducted outreach with key stakeholders; published a notice of proposed rulemaking on how Secure Flight is to operate; and issued a guide to key stakeholders (e.g., air carriers and CBP) that defines, among other things, system data requirements. Collectively, these efforts have enabled TSA to more effectively manage the program's development and implementation.

TSA has also taken steps to integrate the domestic watch-list matching function with the international watch-list matching function currently operated by CBP. We previously reported that TSA was developing Secure Flight to conduct watch-list matching for passengers on domestic flights while, separately, CBP was revising its process for conducting watch-list matching for passengers on flights bound to and from the United States, with limited coordination in their efforts. We reported that this lack of coordination could result in a duplication of effort and conflicting results from domestic and international watch-list matching, as well as create burdens for air carriers who may have been required to operate two separate systems to conduct the domestic and international watch-list matching functions.³⁸ We recommended that DHS take additional steps and make key policy and technical decisions that were necessary to more fully coordinate these programs. TSA and CBP have since worked with DHS to develop a strategy called the One DHS Solution, which is to align the two agencies' domestic and international watch-list matching processes, information technology systems, and regulatory procedures to provide a seamless interface between DHS and the airline industry.³⁹ In line with this

³⁷GAO, *Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System is Further Developed*, GAO-05-356 (Washington, D.C.: March 28, 2005); and GAO, *Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program*, GAO-06-374T (Washington, D.C.: February 9, 2006).

³⁸See GAO-07-448T.

³⁹In August 2007, DHS took two regulatory actions : (1) CBP issued the Advance Passenger Information System (APIS) pre-departure final rule, which requires air carriers to submit passenger manifest information for international flights departing from or arriving in the United States to CBP prior to securing the aircraft (72 Fed. Reg. 48,320 (Aug. 23, 2007));

strategy, the agencies have agreed that TSA will take over international watch-list matching from CBP, with CBP continuing to perform, among other things, its border-related functions. Further, TSA and CBP have coordinated their efforts to facilitate consistency across their programs. For example, in August 2007, they jointly developed and issued a user's guide to the airlines and other stakeholders specifying the data that agencies will need to request from passengers in the future to minimize the impact on systems programming due to the integration of the two programs. TSA and CBP officials plan to pursue further integration as they progress towards developing and implementing the watch-list matching function for international flights.

TSA has also taken steps to address key privacy principles in plans to protect private passenger information for the Secure Flight program. We previously reported that TSA, as part of its requirements development process, had not clearly identified the privacy impacts of the Secure Flight system or the full actions it planned to take to mitigate them. Specifically, we reported that TSA had not made final determinations about its requirements for passenger data, and the program's systems development documentation did not fully address how passenger privacy protections were to be met and, as a result, it was not possible to assess potential system impacts on individual privacy protections. We also reported that TSA violated provisions of the Privacy Act by not fully disclosing its use of personal information during systems testing.⁴⁰ In March 2005, we recommended that TSA specify how Secure Flight will protect personal privacy.⁴¹ In August 2007, TSA published, for public comment, the required privacy impact assessment⁴² and system of records notice⁴³ that address

and (2) TSA issued the Secure Flight Notice of Proposed Rulemaking (NPRM), which identifies DHS' plans to assume watch-list matching responsibilities from air carriers for domestic flights. (72 Fed. Reg. 48,356 (Aug. 23, 2007)).

⁴⁰See GAO, *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*, GAO-05-864R (Washington, D.C.: July 22, 2005).

⁴¹See GAO-05-356.

⁴²The E-Government Act of 2002 requires agencies to conduct privacy impact assessments (PIA). Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921-23 (2002). A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. Agencies are required to make their PIAs publicly available.

key privacy protection principles. For example, these notices describe the information that will be collected from passengers and air carriers, as well as the purpose and planned uses of the data to be collected.⁴⁴ TSA also developed a Program Privacy Architecture describing key aspects of TSA's plans to protect private passenger information, such as embedding privacy experts into program teams, developing privacy requirements documentation, and implementing technical controls to protect privacy such as network security controls. We will continue to monitor their efforts as part of our ongoing work to ensure that privacy protections continue to be appropriately considered.

TSA Has Not Fully Followed Best Practices for Developing Reliable and Valid Cost and Schedule Estimates for Secure Flight

Although TSA has developed a life-cycle cost estimate and maintains an integrated master schedule for Secure Flight, the program has not fully followed best practices for developing reliable and valid cost and schedule estimates, and several program milestones have been missed or have slipped. The Office of Management and Budget (OMB) endorsed the use⁴⁵ of GAO's Cost Assessment Guide in the development of life-cycle cost and program schedule estimates.⁴⁶ The ability to generate reliable cost and schedule estimates is a critical function necessary to support OMB's capital programming process. Without adhering to these best practices in the development of its cost and schedule estimates, TSA is at risk of the Secure Flight program experiencing cost overruns, missed deadlines, and performance shortfalls.

⁴³The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records and requires agencies to publish a public notice, known as a System of Records Notice (SORN), in the Federal Register. See 5 U.S.C. § 552a.

⁴⁴TSA will not issue final notices until it completes its evaluation of public comments on notice of proposed rulemaking. The comment period for the Secure Flight rulemaking closed on November 21, 2007.

⁴⁵OMB's Capital Programming Guide (Supplement to Office of Management and Budget Circular A-11, Part 7: Planning, Budgeting, and Acquisition of Capital Assets) identifies that there are certain key criteria that OMB will look for in the justification of spending for proposed new capital assets including credible cost estimates. Appendix 9 of the guide identifies that following the guidelines in GAO's Cost Assessment Guide will help agencies meet most cost estimating requirements.

⁴⁶See GAO, *Cost Assessment Guide: Best Practices for Estimating and Managing Program Costs, Exposure Draft*, GAO-07-1134SP (Washington, D.C.: July 2007).

Life-cycle cost estimate. We found that TSA has not fully followed best practices for developing a reliable and valid life-cycle cost estimate. Using our Cost Assessment Guide's 12-step process for creating cost estimates, we assessed the Secure Flight cost estimate against these best practices. The Guide outlines a 12-step process, which if followed correctly, should result in high quality, reliable, and valid cost estimates.⁴⁷ DHS's Cost - Benefit Analysis Guidebook, which TSA program officials stated that TSA used to develop the life-cycle cost estimate for Secure Flight, contains most of the best practices outlined in our Guide. TSA followed some of these practices in developing its cost estimate, including defining the purpose of the program and estimate purpose; identifying many program cost elements, including expenditures for facilities, hardware, and software; and identifying the numbers of staff, their pay, and associated travel and training costs, among other elements. However, it is unclear whether TSA followed other best practices or did not address the practices in developing its estimate. For example, it is unclear whether the cost estimate had been updated to reflect the current program because the detailed support for the estimate was produced between 2004 and 2006, and does not reflect the current program plan. In addition, the cost estimate does not capture all key costs. For example, the estimate does not capture costs beyond 2012 even though the system is expected to be operational beyond that date. Secure Flight's Acquisition Program Baseline states that life-cycle costs will run from FY 2002 through FY 2020 and assumes operations of the program through 2020. The cost estimate documentation also did not provide a step-by-step description of the cost estimating process, data sources, and methods used to develop the underlying cost elements consistent with best practices. Finally, TSA did not analyze the amount of certainty it had in its estimate and an independent cost estimate was not developed to assess the reasonableness of the estimate, consistent with best practices. TSA officials stated that the program's cost figures were updated in 2007 and continue to be updated as changes warrant. Officials further stated that their estimates were prepared in accordance with DHS and OMB guidance and were

⁴⁷ The 12 steps involved in developing a high-quality cost estimating process are 1) define the estimate's purpose, 2) develop the estimating plan, 3) define the program, 4) determine the estimating structure, 5) identify ground rules and assumptions, 6) obtain the data, 7) develop the point estimate and compare it to an independent cost estimate, 8) conduct sensitivity analysis, 9) conduct risk and uncertainty analysis, 10) document the estimate, 11) present estimate to management, and 12) update the estimate to reflect actual costs and changes.

reviewed and approved by DHS and OMB. However, without adhering to the best practices discussed above, as recommended by OMB, TSA's cost estimate may not provide a meaningful baseline from which to track progress, and effectively support investment decision making.

Schedule estimate. We found that TSA also did not fully follow best practices for developing a reliable and valid schedule estimate. GAO's Cost Assessment Guide includes 9 best practices, which if followed correctly, should result in high quality, reliable, and valid schedule estimates.⁴⁸ Without a reliable schedule baseline and careful monitoring of its status, a program may not be able to determine when forecasted completion dates differ from planned dates. TSA has made progress in developing a reliable and valid schedule estimate, including capturing key activities and accounting for the development of program requirements and testing. However, TSA officials could not provide evidence that their scheduling software can produce a critical path (i.e., the longest path of sequential activities in a schedule) driven by discrete lower level tasks. Best practices call for the critical path to be generated using scheduling software. We also found that the schedule is not fully integrated because several lower level activities were not connected in a logical manner, as called for by best practices. As a result, the Secure Flight schedule estimate may not provide a meaningful benchmark from which to gauge progress, identify and address potential problems, and make informed decisions. For example, the inability to institute a reliable schedule could affect TSA's ability to effectively measure contractor performance in meeting deliverables. TSA officials stated that their scheduling software can create a critical path, and that lower level tasks in their schedule were logically linked together; however, they did not provide evidence that supported this.

Since TSA completed a re-baselining of the Secure Flight program, and began using its current schedule, the program has missed milestones and experienced schedule slippages. For example, while TSA reports that it

⁴⁸The 9 best practices are 1) capturing key activities, 2) sequencing key activities, 3) establishing the duration of key activities, 4) establishing the critical path for key activities, 5) assigning resources to key activities, 6) identifying "float time" between key activities, 7) distributing reserves to high risk activities (including conducting an independent cost estimate), 8) integrating key activities horizontally--to link products and outcomes associated with already sequenced activities--and vertically--to ensure that traceability exists among varying levels of activities and supporting tasks, and 9) completing schedule risk analysis.

has met most of its March 2007 schedule milestones to date, the August 2007 milestone for developing memoranda of understanding and other written agreements (e.g. service level agreements) with key Secure Flight stakeholders (e.g. CBP) was missed and has not yet been met. TSA officials attributed schedule slippages in part to an extension in the Secure Flight rulemaking comment period and underestimating the time needed to complete key activities. In addition, TSA has not conducted a schedule risk analysis to determine the level of confidence it has in meeting the system's completion date, and has not conducted a cost and schedule risk assessment, consistent with best practices. The cost and schedule risk assessment recognizes the inter-relationship between schedule and cost and captures the risk that schedule durations and cost estimates may vary due to, among other things, limited data, optimistic estimating, technical challenges, lack of qualified personnel, and too few staff to do the work. Without these assessments, TSA has less assurance that it is effectively managing risk associated with Secure Flight's cost and schedule. We will continue to assess TSA's life-cycle cost and schedule estimates as part of our ongoing review of the Secure Flight Program.

TSA Has Made Progress in Strengthening Secure Flight's Development, but Can Further Strengthen Efforts

While TSA has taken numerous steps to strengthen the development of Secure Flight, additional challenges remain. These challenges include: 1) implementing the program's risk management plan, 2) planning and conducting end-to-end testing as part of their overall parallel testing strategy, and 3) addressing information security requirements and vulnerabilities.

Risk management. In October 2006, TSA issued a risk management plan for identifying, managing, and mitigating Secure Flight program risks that was consistent with relevant guidance and best practices. TSA also acquired an electronic tool to guide its risk management efforts. However, TSA has not yet provided us with evidence that it has implemented all aspects of the plan, including developing an inventory of risks and related information to demonstrate that its risk management tool has been populated and is being used to identify, prioritize, mitigate, and monitor risk. Federal guidance and related best practices recognize the importance of proactively managing risks during systems development and implementation,⁴⁹ and advocate a program's use of a risk management

⁴⁹See, for example, Software Engineering Institute, *Capability Maturity Model Integration (CMMI) for Development, Guidelines for Process Integration and Product Improvement*, Second Edition, Version 1.2 (May 2007).

plan. However, although TSA developed a risk management plan, the agency only recently, in December 2007, established a risk management board to manage program risks as called for by the plan. TSA officials stated that the risk management board has met three times since December 2007, and, in January 2008, compiled an updated and consolidated inventory of all program risks, including ranking and mitigation strategies. However, TSA officials have not provided us with documentation identifying the board's activities and resulting risk inventory. Prior to December 2007, in lieu of a formal risk management board, program officials stated that each project team addressed risks as part of biweekly project management meetings. However, we found these efforts to be limited in that the risks discussed did not include priority rankings such as probability and impact, and many did not have mitigation strategies, as required by the program's risk management plan. In November 2007, TSA hired a risk management coordinator, a position that had been vacant since June 2007. According to program officials, the coordinator has been tasked with supporting the risk management board in implementing the risk management plan and has provided related training for its members. Secure Flight officials stated that although they have not fully implemented their risk management plan, they believe that they are effectively managing program risks through the methods previously discussed, and that over the past few months, have enhanced their risk management efforts. However, until the risk management plan is appropriately implemented, there is an increased chance that program risks will not be proactively mitigated and may result in program cost overruns, and schedule and performance shortfalls. We will continue to assess TSA's efforts to manage risk as part of our ongoing review of Secure Flight.

End-to-end test planning. Secure Flight does not fully outline plans for end-to-end testing in its overall test and evaluation plan, or other test plans. Federal guidance and related best practices recommend end-to-end testing to verify that the systems that collectively support a program like Secure Flight will interoperate as intended in an operational environment, either actual or simulated.⁵⁰ We reported in March 2005 on the importance of Secure Flight end-to-end testing and recommended that TSA perform such testing.⁵¹ TSA agreed with this recommendation. However, Secure

⁵⁰Risks of testing in the production environment must be thoroughly analyzed and precautions taken to preclude damage to systems and data. See GAO, *Year 2000 Computing Crisis: A Testing Guide*, GAO/AIMD-10.1.21 (Washington, D.C.: November 1998).

⁵¹See GAO-05-356.

Flight's current test and evaluation master plan only outlines plans for partner organizational entities (e.g., CBP for integration of international watch-list functions) to test their respective parts of the system on their own—rather than a coordinated end-to-end test involving all parties. TSA developed a preliminary working draft of an end-to-end testing strategy, called the parallel testing strategy. However, the plan does not contain provisions for (1) testing that ensures that supporting systems will operate as intended in an operational environment, (2) definitions and dates for key milestone activities and parties responsible for completing them, or (3) the revision of other test plans, such as the test and evaluation master plan, to reflect the performance of end-to-end tests. Secure Flight officials stated that they plan to conduct full end-to-end testing of the program, beginning in the Spring of 2008, and that they will reflect this testing in test plans that are still under development. While we commend TSA's plans to conduct end-to-end testing, the draft of TSA's test plan that discusses end-to-end testing does not define a scope that extends to all aspects of the program. Until TSA has well-defined and approved end-to-end test plans and procedures, it will be challenged in its ability to demonstrate that Secure Flight will perform in a way that will allow it to achieve intended program outcomes and results. We will continue to assess TSA's testing strategy, to include end-to-end testing, as part of our ongoing review of the program.

Information security. While the Secure Flight program office has completed important steps to incorporate security into the system's development, it has not fully completed other steps to ensure security is effectively addressed. Federal standards and guidance identify the need to address information security throughout the life-cycle of information systems, and specifies a minimum set of security steps needed to effectively incorporate security into a system during its development.⁵² The Secure Flight program has performed several steps that incorporate security into the system's development, including performing a security risk assessment, identifying and documenting recommended security control requirements, and testing and evaluating security controls for the system and incorporating identified weaknesses in remedial action plans. However, other steps pertaining to ensuring that security requirements are tested, preparing security documentation, and conducting certification and

⁵²National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce, *Security Considerations in the Information System Development Life-Cycle*, NIST Special Publication 800-64 (Gaithersburg, Md: June 2004).

accreditation activities were not adequately completed.⁵³ For example, security requirements planned for Release One did not always trace to test activities for this release.⁵⁴ Program officials stated that some security requirements were deferred until future releases due to delays in funding for acquiring specific hardware and other requirements require coordination with the information system security official to verify whether they were tested as part of security test and evaluation. In addition, security documentation contained incorrect or incomplete information. To illustrate, the systems security plan did not identify all interconnecting systems that Secure Flight will interface with, such as those operated by the DHS Watch-List Service, the organization that will transmit the watch-list to Secure Flight. Program officials stated that security documentation was outdated or incorrect because there was insufficient time to update the documentation for changes in the computing environment and security requirements.

Furthermore, program officials granted an authorization to operate—one of three possible accreditation decisions made in the certification and accreditation process—although the system had 46 known vulnerabilities, including 11 high-risk and 27 moderate-risk vulnerabilities and the controls had not yet been implemented.⁵⁵ Federal guidance as well as DHS policy provide for an interim authority to operate accreditation when significant restrictions or limitations exist and certain deficiencies and corrective actions need to be addressed within a specified period. Although security officials identified plans of actions and milestones for addressing the vulnerabilities within 60 and 90 days for the high and moderate risks, respectively, given their significance, an interim authorization to operate

⁵³OMB requires that agency management officials formally authorize their information systems to process information and accept the risk associated with their operation. This management authorization (accreditation) is to be supported by a formal technical evaluation (certification) of the management, operational, and technical controls established in an information system's security plan. See GAO, *Information Security: Although Progress Reported, Federal Agencies Need to Resolve Significant Deficiencies*, GAO-08-496T, (Washington, D.C.: February 14, 2008).

⁵⁴These activities include 1) system testing performed as part of software development, and 2) security test and evaluation performed as part of certification and accreditation.

⁵⁵TSA defines high-risk vulnerabilities as those where there is a strong need for corrective measures, the probability of serious incident is likely and risks are not normally acceptable, corrective action plans must in place as soon as possible, and the authorization to operate may be receded or not granted. Moderate-risk vulnerabilities are those where the probability of incident is elevated, with increased probability of unauthorized disclosure or disruption of operations, and risks are probably not acceptable.

would be the more appropriate determination. In addition, hardware components used to implement controls over user identity and account management (i.e., authentication, logins and passwords, and user roles and privileges), as well as the alternate processing site had not yet been implemented. Once implemented, the security controls over these components could have an impact on the information security and, therefore, may require a re-accreditation. Program officials chose the authority to operate accreditation because they asserted that the DHS Chief Information Security Officer does not allow interim authorizations. If these security activities are not completed, there is an increased risk that key security controls and requirements may not be fully developed, tested, implemented or documented.

DHS and TSA Lack Performance Measures to Fully Evaluate the Effectiveness of the Redress Process, But Plan Additional Measures under Secure Flight

DHS and TSA have not developed a complete set of performance measures to assess the effectiveness of the redress process for passengers inconvenienced as a result of watch-list matching.⁵⁶ Measuring performance allows organizations to track the progress they are making toward their goals and gives managers critical information on which to base decisions for improving their programs. DHS and TSA are developing additional measures for the redress process that they plan to implement when Secure Flight becomes operational.

TSA, supported by the Terrorist Screening Center, provides opportunities for airline passengers to seek redress in cases where they experienced inconveniences during the check-in and screening processes due to the possibility they have been misidentified as being on or wrongly assigned to the terrorist watch-list.⁵⁷ The redress process enables these individuals to file an inquiry to have erroneous information corrected in DHS systems that may prevent future delays and inconveniences at the airport. In February 2007, DHS established the Traveler Redress Inquiry Program (TRIP) to serve as the central processing point within the department for redress inquiries. TSA's Office of Transportation Security Redress (OTSR) is responsible for reviewing redress inquiries submitted by air passengers through TRIP. According to a DHS official, in addition to handling redress applications, TRIP officials review, attempt to address, and respond to

⁵⁶In general, performance measures are indicators, statistics, or metrics used to gauge program performance.

⁵⁷The term "misidentified" refers to a person initially matched by a screening entity to a name on the watch-list, but upon closer examination, the person is found to not match any watch-list record.

written complaint letters received from individuals who have gone through the redress process but are still experiencing screening issues.

TRIP and OTSR's redress program goals are to process redress applications as quickly and as accurately as possible. However, to measure program performance against these goals, TRIP and OTSR currently track only one measure for redress related to the timeliness of case completion, and do not track any performance measures related to program accuracy. Previous GAO work identified that agencies successful in evaluating performance had measures that used attributes from GAO's best practices.⁵⁸ Specifically, our previous work identified that agencies successful in evaluating performance had measures that demonstrated results, covered multiple priorities, provided useful information for decision making, and successfully addressed important and varied aspects of program performance. TRIP and OTSR officials stated that they do not plan to develop additional performance measures, such as measures related to accuracy of the redress process, but rather are awaiting the implementation of Secure Flight to determine the program's impact on the redress process before creating additional measures. Secure Flight is intended to reduce the inconveniences experienced by air passengers by taking over from air carriers the responsibility for prescreening passengers in order to ensure consistent and effective use of the cleared list,⁵⁹ which should impact the effectiveness of the redress process.⁶⁰

In addition to TRIP and OTSR's performance measures for the redress process, the Secure Flight program office is working with OTSR to develop redress performance measures for the Secure Flight Program. As we reported in February 2007, Secure Flight will use the TSA redress process that is currently available for individuals affected by the air carrier identity-matching processes. Secure Flight is coordinating with OTSR to determine how this process will be integrated with other Secure Flight

⁵⁸GAO, *Tax Administration: IRS Needs to Further Refine Its Tax Filing Season Performance Measures*, GAO-03-143, (Washington, D.C.: November 22, 2002).

⁵⁹The cleared list contains the names and other personal identifying information of individuals who have gone through the redress process and have been checked and cleared as being persons not on the No Fly or Selectee lists.

⁶⁰Under Secure Flight, as described by TSA's notice of proposed rulemaking, TSA plans to introduce a unique redress number that would enable Secure Flight to "pre-clear" individuals who have previously been misidentified, have gone through the redress process, and who provide additional identifying information when making a reservation. TSA expects this to reduce the likelihood of travel delays at check-in for those passengers.

requirements. Secure Flight and OTSR are jointly developing a set of performance measures and targets covering multiple priorities for redress that are to be implemented when Secure Flight becomes operational, and officials told us that they will follow best practices in the development of these measures.

While we commend TSA for developing redress performance measures for the Secure Flight Program, since the program is not scheduled to be implemented until January 2009, DHS and OTSR's current redress process lacks a complete set of measures with which they can assess performance and make program improvements. Since measures are often the key motivators of performance and goal achievement, the program's overall success is at risk if all priorities are not addressed and information is not obtained to make future adjustments and improvements to the program. By developing and implementing measures that address all program goals now, to include measures related to program accuracy, DHS and TSA would have performance data that would allow them to better manage the redress process in place today, identify and correct any weaknesses, and help to ensure accountability towards the traveling public that the process is effective. Moreover, such performance data would provide a baseline against which to benchmark Secure Flight's progress and planned improvements to the redress process.

Conclusions

DHS and TSA have undertaken numerous initiatives to strengthen the security of the nation's aviation system, and should be commended for these efforts. More specifically, TSA developed processes to more efficiently allocate and deploy the TSO workforce, strengthened screening procedures, is working to develop and deploy more effective screening technologies, strengthened the security of air cargo, and improved the development of a program to prescreen passengers against the terrorist watch-list. However, opportunities exist to further strengthen these efforts, in particular in the areas of risk management and program planning and monitoring. Our work has shown—in homeland security and in other areas—that a comprehensive risk management approach can help inform decision makers in the allocation of finite resources to the areas of greatest need. We are encouraged that risk management has been a cornerstone of DHS and TSA policy, and that TSA has implemented risk-based decision making into a number of its efforts. Despite this commitment, however, TSA will continue to face difficult decisions and trade-offs—particularly as threats to commercial aviation evolve—regarding acceptable levels of risk and the need to balance security with efficiency and customer service. We recognize that doing so will not be

easy. In implementing a risk-based approach, DHS and TSA must also address the challenges we identified in our work related to program planning and monitoring. Without rigorous planning and monitoring, and knowledge of the effectiveness of aviation security programs implemented, DHS and TSA cannot be sure that they are focusing their finite resources on the areas of greatest need, and that security programs implemented are achieving their desired purpose.

One area in which TSA has made considerable progress is in the development and implementation of the Secure Flight Program. Since we last reported on the program in February 2007, TSA has instilled more discipline and rigor into the systems development, and has completed key development and privacy protection activities. Despite this progress, however, it is important that TSA continue to work to strengthen the management of the program. TSA needs to take immediate and strong actions to keep the program on track and increase the likelihood that it will successfully implement Secure Flight on time, within budget and meeting all performance expectations. We found that TSA did not fully follow best practices for developing Secure Flight's life-cycle cost and schedule estimates. The ability to generate reliable cost and schedule estimates is a critical function necessary to support the Office of Management and Budget capital programming process. Without adhering to these best practices in the development of its cost and schedule estimates, TSA is at risk of the Secure Flight Program experiencing cost overruns, missed deadlines, and performance shortfalls. In order to help inform management's decisions regarding the program and assist them in providing effective program oversight, it is also important that TSA fully implement the provisions in the program's risk management plan to include developing an inventory of risks and reporting the status of risks to management. TSA should also work to plan for complete end-to-end testing of the system to ensure that all interrelated components operate as intended, and strengthen key security controls and activities for the program, including ensuring that security requirements are tested and implemented, and that security documentation is maintained and updated. It is also important that TSA ensure that security risks are addressed in action plans, and that security risks are appropriately monitored so that the system is protected from unauthorized users and abuse. Finally, with respect to passenger redress, DHS and TSA should more thoroughly assess the effectiveness of the current redress process, to include the development of additional performance measures that assess program accuracy, a key goal of the program.

Recommendations for Executive Action

To assist TSA in further strengthening the development and implementation of the Secure Flight program, we recommend that the Secretary of Homeland Security direct the Assistant Secretary of the Transportation Security Administration to take the following three actions:

- Fully incorporate best practices into the development of Secure Flight life-cycle cost and schedule estimates, to include:
 - updating life-cycle cost and schedule estimates;
 - demonstrating that the Secure Flight schedule has the logic in place to identify the critical path, integrates lower level activities in a logical manner, and identifies the level of confidence in meeting the desired end date; and
 - developing and implementing a plan for managing and mitigating cost and schedule risks, including performing a schedule risk analysis and a cost and schedule risk assessment.
- Fully implement the provisions in the program's risk management plan to include developing an inventory of risks with prioritization and mitigation strategies, report the status of risks and progress to management, and maintain documentation of these efforts.
- Finalize and approve Secure Flight's end-to-end testing strategy, and incorporate end-to-end testing requirements in other relevant test plans, to include the test and evaluation master plan. The strategy and plans should contain provisions for:
 - testing that ensures that the interrelated systems that collectively support Secure Flight will interoperate as intended in an operational environment; and
 - defining and setting dates for key milestone activities and identifying who is responsible for completing each of those milestones and when.

We further recommend that the Secretary of Homeland Security direct the TSA Chief Information Officer to take the following three actions regarding information security for the Secure Flight Program:

- coordinate with Secure Flight program officials to ensure security requirements are tested and implemented;
- maintain and update security documentation to align with the current or planned Secure Flight computing environment, including

interconnection agreements, in support of certification and accreditation activities; and

- correct identified high and moderate risk vulnerabilities, as addressed in remedial action plans, and assess changes to the computing environment to determine whether re-accreditation of the system is warranted.

Finally, to ensure that DHS is able to fully assess the effectiveness of the current redress process for passengers who may have been misidentified during the watch-list matching process, we recommend that the Secretary of Homeland Security and the Assistant Secretary of the Transportation Security Administration re-evaluate redress performance measures and consider creating and implementing additional measures that, consistent with best practices, demonstrate results, cover multiple priorities, and provide useful information for decision making. These measures should further address all program goals, to include the accuracy of the redress process.

Agency Comments and Our Evaluation

We provided a draft of information included in this statement related to our recently completed work on Secure Flight to DHS and TSA for review and comment. We incorporated technical changes to this statement based on TSA's comments. In commenting on this information, DHS and TSA generally agreed with our recommendations.

Contacts and Acknowledgements

For further information on this testimony, please contact Cathleen A. Berrick at (202) 512-3404 or berrickc@gao.gov, or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

In addition to the contacts named above, Don Adams, Idris Adjerid, Kristy Brown, Chris Currie, Katherine Davis, John DeFerrari, Joe Dewechter, Jennifer Echard, Eric Erdman, Randolph Hite, James Houtz, Anne Laffoon, Thomas Lombardi, Gary Malavenda, Steve Morris, Sara Margraf, Vernetta Marquis, Vickie Miller, Gary Mountjoy, David Plocher, Jamie Pressman, Karen Richey, Karl Seifert, Maria Strudwick, Meg Ullengren, Margaret Vo, and Jenniffer Wilson made contributions to this testimony.
