United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Aviation, Committee on Commerce, Science and Transportation, U.S. Senate

For Release on Delivery
Expected at 9:30 a.m. EST
Tuesday, March 30, 2004

AVIATION SECURITY

Improvement Still Needed in Federal Aviation Security Efforts

Statement of Norman J. Rabkin
Managing Director, Homeland Security and Justice Issues

March 2004

AVIATION SECURITY

Improvements Still Needed in Federal Aviation Security Efforts

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-592T, a testimony before the Subcommittee on Aviation, Committee on Commerce, Science and Transportation, U.S. Senate

Why GAO Did This Study

The security of the nation's commercial aviation system has been a long-standing concern. Following the events of September 11, 2001, Congress enacted numerous aviation security improvements designed to strengthen aviation security, including the development of a passenger prescreening system and the federalization of airport screeners. Despite these changes, challenges continue to face the Department of Homeland Security (DHS) and the Transportation Security Administration (TSA) efforts to improve aviation security. GAO was asked to summarize the results of previous and ongoing aviation security work. These include: (1) the development of CAPPS II to assist in identifying high-risk passengers, (2) the management of passenger and baggage screening programs, (3) the operations of the Federal Air Marshal Service, and (4) other aviations security related efforts, such as cargo, that remain a concern.

What GAO Recommends

In prior reports and testimonies, listed at the end of this statement, GAO has made recommendations to improve aviation security and to strengthen various security efforts underway. We also have several ongoing reviews assessing certain issues addressed in this testimony that will be published under separate reports at a later date.

www.gao.gov/cgi-bin/getrpt?GAO-04-592T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Norman J. Rabkin at (202) 512-8777 or rabkinn@gao.gov.

What GAO Found

Numerous challenges continue to face TSA in its efforts to improve the nation's aviation security system. First, key activities in the development of CAPPS II have been delayed and TSA has not yet completed important system planning activities. TSA is behind schedule in testing and developing initial increments of CAPPS II due to delays in obtaining needed passenger data for testing from air carriers because of privacy concerns and has not established a complete plan identifying specific system functionality to be delivered, the schedule for delivery, and estimated costs. TSA also has not fully addressed seven of eight issues identified by Congress as key elements related to the development, operation, and public acceptance of CAPPS II. Additionally, three other major challenges—international cooperation, program mission expansion, and identity theft—need to be adequately addressed to ensure CAPPS II's successful implementation.

Second, TSA continues to face challenges in hiring, deploying, and training its screener workforce. Staffing shortages and TSA's hiring process continue to hinder its ability to fully staff screening checkpoints without using additional measures, such as mandatory overtime. Further, TSA continues to have difficulty deploying and leveraging screening equipment and technologies because of competing priorities in a tight budget environment.

Third, the rapid expansion of the Federal Air Marshal Service has encountered a number of operational and management problems. To accommodate the expansion, the Service revised and abbreviated its training curriculum. The Service developed an advanced training course for newly hired marshals to provide additional skills but funding cutbacks have delayed completion of this training for all air marshals. Most recently, budget constraints have not permitted the Service to reach its target staffing levels and are delaying efforts to develop its field location infrastructure and its automated system to schedule air marshal missions.

Fourth, DHS and TSA face other challenges as they continue to address threats to the nation's aviation system. Significant challenges include developing measures to counter the growing concerns over portable surface-to-air missiles, improving airport perimeter and access controls, and addressing security concerns related to air cargo and general aviation.

Screening Passengers and Cargo are Aviation Security Concerns.

Source: FAA.

Source: Cargo King, Ltfd.

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to participate in today's hearing to discuss the security of our nation's aviation system and the numerous efforts under way to improve it. Protecting the nation's air transportation system is an evolving process that requires continuously adjusting protective measures to meet the ever-changing nature of terrorist threats. Since the late 1960s and early 1970s when passenger screening was first initiated, increasing and improving aviation security has been a learning experience. Each incremental increase in security was usually the result of some catastrophic event, the most recent being the September 11, 2001, attacks. Following that tragic event, aviation security efforts have been refocused and reorganized through the creation of the Department of Homeland Security (DHS) and the Transportation Security Administration (TSA), the strengthening of federal leadership and responsibility for aviation security, and the funding of billions of dollars each year for programs and initiatives to maintain and enhance aviation security. Yet despite this large and focused effort, concerns over the security of our aviation system remain.

My testimony today focuses on DHS's and TSA's aviation security efforts in four areas: (1) the development of the new Computer-Assisted Passenger Prescreening System (CAPPS II) to help identify high-risk passengers prior to arriving at the airport, (2) the management by TSA of its passenger and baggage screening programs, (3) the operation of the Federal Air Marshal Service, and (4) other aviation security-related efforts that remain a concern. This testimony is based on our prior and ongoing work and review of recent literature. A listing of our prior reports is contained in appendix I.

In summary, we found that:

- Key activities in the development of CAPPS II have been delayed and TSA has not completed important system planning activities. TSA is behind schedule in testing and developing the system's initial increments due to delays in obtaining passenger data needed for testing from air carriers because of privacy concerns, and it has not established an overall plan identifying specific system functionality that will be delivered, the schedule for delivery, and estimated costs. TSA also has not completely addressed seven of the eight issues identified by the Congress as key areas of interest related to the development, operation, and public acceptance of CAPPS II. Additionally, there are three major challenges—international cooperation, program mission

expansion, and identity theft—that could prevent the successful implementation of CAPPS II if not adequately resolved by TSA.

- TSA continues to face challenges in hiring, deploying, and training its screener workforce even though it met the mandate to establish a federal screener workforce by November 2002. Staffing shortages and TSA's hiring process continue to hinder its ability to fully staff screening checkpoints without using additional measures, such as mandatory overtime. Additionally, TSA has taken steps to enhance its screener training programs, but staffing shortages and lack of high-speed connectivity at many airport training facilities have made it difficult for screeners to fully utilize these programs. Further, TSA continues to face challenges in deploying and leveraging screening equipment and technologies because of competing priorities in a tight budget environment.

- The rapid expansion of the Federal Air Marshal Service has encountered a number of operational and management problems. In order to deploy its expanded workforce by July 1, 2002, the Service developed an advanced training course to provide additional training for newly hired air marshals, but funding cutbacks have delayed expected completion of this training by all air marshals until mid-2004. More recently, because of budget constraints, Service officials said that the number of air marshals has not reached target levels and may be declining, equipment and facilities for field locations cannot be obtained, and the development of systems to schedule and manage air marshal missions have been delayed.

- DHS and TSA face a number of other challenges as they continue to address threats to the nation's aviation system. Significant challenges include developing measures to counter the growing concerns over portable shoulder-launched surface-to-air missiles, improving airport perimeter and access controls, and addressing broad security concerns related to air cargo and general aviation. We have work in progress that is examining these issues.

Background

The security of the U.S. commercial aviation system has been a long-standing concern. Over the years, numerous initiatives have been implemented to strengthen aviation security. However, as we and others have documented in numerous reports and studies, weaknesses continue to exist. It was due in part to these weaknesses that terrorists were able to hijack four commercial aircraft on September 11, 2001, with tragic results. Concerns continue to exist regarding the security of the aviation system, as evidenced by the cancellations of several, mostly transatlantic flights to

and from the United States in response to intelligence information regarding specific threats to those flights.

With hundreds of commercial airports, thousands of commercial aircraft, tens of thousands of daily flights, and millions of passengers using the system daily, providing security to the nation's commercial aviation system is a daunting task. In an effort to strengthen the security of commercial aviation, the President signed into law the Aviation and Transportation Security Act (ATSA) on November 19, 2001.[1] ATSA created TSA and mandated actions designed to strengthen aviation security, including the federalization of passenger and baggage screening at over 440 commercial airports in the United States by November 19, 2002, and the screening of all checked baggage using explosive detection systems. On March 1, 2003, pursuant to the Homeland Security Act of 2002,[2] TSA was transferred from the Department of Transportation to the newly created Department of Homeland Security.

Virtually all aviation security responsibilities now reside within DHS, and most of these are with TSA, including conducting passenger and baggage screening, and overseeing security measures for airports, commercial aircraft, air cargo, and general aviation. Only the Federal Air Marshal Service, which was recently moved from TSA to DHS's Bureau of Immigration and Customs Enforcement, is not within the responsibilities of TSA. Taken together, these programs are intended to form a layered system that maximizes the security of passengers, aircraft, and other elements of the aviation infrastructure.

Significant Challenges Face Implementation Of Computer-Assisted Passenger Prescreening System

One effort under way to strengthen aviation security is TSA's development of a Computer-Assisted Passenger Prescreening System, known as CAPPS II, to replace the current prescreening system now in use. CAPPS II will evaluate each passenger's level of risk before they reach the check-in counter at the airport by accessing commercial and government databases to authenticate the passenger's identity and generate a risk score. The risk scores will be used to determine if passengers need additional security measures or, if warranted, be denied boarding and/or detained by law enforcement.

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

[2]Pub. L. No. 107-296, 116 Stat. 2135.

However, as we recently reported, TSA faces numerous challenges that could affect CAPPS II's successful development and implementation.[3] Key activities in the development of CAPPS II are behind schedule and TSA has not developed critical system plans; numerous developmental, operational, and privacy issues of concern to the Congress remain unresolved by TSA; and other significant challenges exist that could affect the successful implementation of CAPPS II. As a result, the potential for CAPPS II to improve aviation security remains questionable until TSA addresses the numerous concerns raised and challenges facing the program.

Program Delays and Critical Plans Incomplete

Key activities in the development of CAPPS II have been delayed and TSA has not yet completed critical system planning activities. TSA is developing CAPPS II in nine increments, with each increment providing increased functionality. As each increment reached completion, TSA planned to conduct tests that would ensure the system meets the objectives of that increment before proceeding to the next increment. The development of CAPPS II began in March 2003 with increments 1 and 2 being completed in August and October 2003, respectively. However, TSA has not completely tested these initial two increments because it was unable to obtain the necessary passenger data for testing from air carriers. Air carriers have been reluctant to provide passenger data due to privacy concerns. As a result, TSA deferred completing these tests until increment 3.

Completion of increment 3, however, has been delayed. Due to the continued inability to secure passenger data for testing, TSA delayed the completion of increment 3 from October 2003 until the end of March 2004. Moreover, the functionality that this increment was expected to achieve has been reduced. Increment 3 was originally intended to provide a functioning system that could handle live passenger data from one air carrier in a test environment to demonstrate that the system can satisfy operational and functional requirements. However, TSA officials reported that they recently modified increment 3 to instead provide a functional application of the system in a simulated test environment that is not actively connected to an airline reservation system, and they are uncertain

[3]U.S. General Accounting Office, *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385 (Washington, D.C.: Feb. 12, 2004).

when testing that was deferred from increments 1 and 2 to increment 3 will be completed. As a result, all succeeding increments of CAPPS II have been delayed.

Further, TSA has not yet developed critical elements associated with sound project planning, including a plan for what specific functionality will be delivered, by when, and at what cost throughout the development of the system. For example, although TSA established plans for the initial increments of the system, it lacks a comprehensive plan identifying the specific functions that will be delivered during the remaining increments; such as, which government and commercial databases will be incorporated, the date when these functions will be delivered, and an estimated cost of the functions. In addition, TSA officials are uncertain when CAPPS II will achieve initial operating capability—the point at which the system will be ready to operate with one airline. Project officials also said that because of testing delays, they are unable to plan for future increments with any certainty. Until project officials develop a plan that includes scheduled milestones and cost estimates for key deliverables, CAPPS II is at increased risk of not providing the promised functionality, not being fielded when planned, and being fielded at an increased cost.

Issues Identified by Congress Remain Unresolved

TSA has not fully addressed seven of eight issues identified by the Congress as key areas of interest related to the development and implementation of CAPPS II. At this time, only one issue—the establishment of an internal oversight board to review the development of major systems that includes CAPPS II—has been addressed. DHS and TSA are taking steps to address the remaining seven issues; however, they have not yet

- determined and verified the accuracy of the databases to be used by CAPPS II,
- stress tested and demonstrated the accuracy and effectiveness of all search tools to be used by CAPPS II,
- developed sufficient operational safeguards to reduce the opportunities for abuse,
- established substantial security measures to protect CAPPS II from unauthorized access by hackers and other intruders,
- adopted policies to establish effective oversight of the use and operation of the system,
- identified and addressed all privacy concerns, and

- developed and documented a process under which passengers impacted by CAPPS II can appeal decisions and correct erroneous data.

Although TSA is in various stages of progress to address each of these issues, TSA has not established milestones for some and delayed others without estimating a new completion date. For example, TSA planned to conduct stress and system tests by August 2003; however, stress testing was delayed several times due to TSA's inability to obtain the passenger data needed to test the system. Completion of stress testing was moved to March 31, 2004, but this testing has been postponed again and currently no estimate exists for when these tests will be conducted. Although TSA program officials contend that their ongoing efforts will ultimately address each issue, program officials were unable to identify a time frame for when all remaining issues will be fully addressed.

Other Challenges Could Affect Successful Implementation of CAPPS II

CAPPS II faces three other challenges that, if not adequately resolved, pose major risks to its successful development, implementation, and operation. First, for CAPPS II to operate fully and effectively, it needs data not only on U.S. citizens but also on foreign nationals on all international flights coming to, or departing from, the United States as well as all domestic flights. However, obtaining international cooperation for access to these data remains a substantial challenge. The European Union, in particular, has objected to its citizens' data being used by CAPPS II, whether a citizen of a European Union country flies on a U.S. carrier or an air carrier under another country's flag, because it may violate the civil liberties and privacy rights of its citizens. According to a December 2003 report from the Commission of European Communities, the European Union will not be in a position to agree to the use of its citizens' passenger data for CAPPS II until internal U.S. processes have been completed and it is clear that the U.S. Congress's privacy concerns have been resolved. Discussions with the European Union on this issue are ongoing.

Second, the original purpose of CAPPS II may be expanded and this expansion may in turn affect program objectives and public acceptance of the system. The primary objective of CAPPS II was to protect the commercial aviation system from the risk of foreign terrorism by screening for high-risk or potentially high-risk passengers. However, TSA has said that the system would seek to identify domestic terrorists as well as foreign terrorists and that the system could be expanded to identify persons who are subject to outstanding federal or state arrest warrants for violent crimes and those individuals who are in the United States illegally

or who have overstayed their visas. DHS officials contend that such changes are not an expansion of the system's mission because they believe these additional objectives will improve aviation security and are consistent with CAPPS II's mission. However, concerns exist that expanding CAPPS II's mission could also lead to an erosion of public confidence in the system, increase the costs of passenger screening and the number of passengers erroneously identified as needing additional security attention, and put TSA at risk of diverting attention from the program's fundamental purpose.

Third, the successful operation of CAPPS II depends on the system's ability to effectively identify passengers who assume the identity of another individual. TSA officials said that CAPPS II should detect situations in which a passenger submits fictitious information such as a false address. These instances would likely be detected since the data being provided would either not be validated or would be inconsistent with information in the databases used by CAPPS II. However, the officials acknowledge that some identity theft is difficult to spot, particularly if the identity theft is unreported or if collusion, where someone permits his or her identity to be assumed by another person, is involved. TSA officials said that there should not be an expectation that CAPPS II will be 100 percent accurate in identifying all cases of identity theft, and that although not foolproof, CAPPS II represents an improvement in identity authentication over the current system.

Efforts to Improve Screening Face Challenges

One of the critical layers of our nation's aviation security system is passenger and baggage screening. All passengers on commercial airliners must pass through airport screening checkpoints and have their carry on and checked baggage screened. TSA manages the screening operations and uses electronic searches, manual searches, and other measures to determine if threat objects, including explosives, are in the possession of the passengers or in their baggage. Following the events of September 11, 2001, airline passenger and baggage screening became a federal responsibility and is now carried out by TSA employees or, in the case of five airports, by private screening companies under the direction of TSA.[4]

[4]Consistent with the provisions of ATSA, TSA implemented a pilot program using contract screeners at five commercial airports. The purpose of the 2-year pilot program is to determine the feasibility of using private screening companies rather than federal screeners.

Our recent work on screening has found that numerous challenges impede TSA's progress in improving screening.[5] Four key areas of concern include TSA's efforts to (1) hire and deploy passenger and baggage screeners, (2) train the screening workforce, (3) measure screener performance in detecting threat objects, and (4) leverage and deploy screening equipment and technologies.

Concerns Remain Regarding Hiring and Deploying the Screener Workforce

TSA accomplished a significant goal by hiring and deploying more than 55,000 screeners by November 19, 2002. However, its initial staffing efforts created imbalances in the screener workforce. While some airports had too many screeners, others had too few. To address these imbalances, as well as congressional concerns regarding overall screener-staffing levels, TSA began attempting to right-size its screener workforce. Specifically, TSA established a goal to reduce its screener workforce by 3,000 screeners by June 1, 2003, and an additional 3,000 screeners by September 30, 2003. These reductions were achieved through attrition, voluntary transfers from full to part-time, and involuntary transfers to part-time or terminations based on screeners' scores on competency-based examinations.

However, TSA continues to struggle to achieve the right number of screeners at airport passenger and baggage checkpoints and has not yet achieved a stable screener workforce. To accomplish its security mission, TSA needs a sufficient number of screeners trained and certified in TSA security procedures and technologies. Currently, TSA's screener staffing level is below a congressionally imposed staffing cap of 45,000 full-time equivalents.[6] According to TSA officials, TSA has experienced an average annual attrition rate of 14 percent for screeners, with some of the larger airports reportedly experiencing annual attrition rates ranging from 15 to 36 percent. TSA has also experienced difficulties in hiring new staff. TSA's hiring process is designed to ensure that its hiring practices are standardized and consistent throughout all airports. However, this process has hindered the ability of some Federal Security Directors (FSD)[7] to adequately staff passenger and baggage screening checkpoints. In

[5]U.S. General Accounting Office, *Aviation Security: Challenges Exist is Stabilizing and Enhancing Passenger and Baggage Screening Operations*, GAO-04-440T (Washington, D.C.: Feb. 12, 2004).

[6]One full-time equivalent is equal to one work year or 2,080 non-overtime hours.

[7]FSDs are responsible for overseeing security at each of the nation's commercial airports.

addition, TSA has also experienced challenges in attracting needed part-time screeners. As a result, FSDs at some of the larger airports we visited had to frequently require mandatory overtime, particularly during the holiday season, to accomplish screening functions.

To help right-size and stabilize its screener workforce, TSA hired a consultant in September 2003 to conduct a study of screener staffing levels at the nation's commercial airports. Specifically, the consultant was tasked with, among other things, evaluating TSA's current staffing methodology and systems to establish a baseline, developing a comprehensive modeling approach that accounts for the considerable variability that occurs among airports,[8] integrating modeling parameters into TSA's screener scheduling system, and delivering user friendly simulation software that will determine optimum screener staffing levels for each of the more than 440 commercial airports with federal screeners. TSA expects the consultant's study to be completed in April 2004.

TSA is also trying to compensate for screener shortages and to enable operational flexibility to respond to changes in risk and threat. In October 2003, TSA established a National Screening Force to provide screening support to all airports in times of emergency, seasonal demands, or under other special circumstances that require a greater number of screeners than regularly available to FSDs. The National Screening Force currently consists of over 700 full-time passenger and baggage screeners, of which about 10 percent are screening supervisors. TSA officials said that they determine where to deploy members of the National Screening Force based on priorities. For example, the highest priority is given to those airports that need additional screeners in order to be able to screen 100 percent of checked baggage using Explosive Detection Systems (EDS) and Explosive Trace Detection (ETD) systems. TSA is also currently drafting standard operating procedures for the National Screening Force. We have ongoing work that will examine TSA's use of the National Screening Force and other staffing issues.

[8]TSA officials said that it required the contractor to validate the staffing model using statistical samples of all staff and equipment operations at all category X airports and as many category I, II, III, and IV airports as necessary.

Screener Training Programs Enhanced, but Access to Programs Is Sometimes Limited

TSA has taken steps to enhance its training programs for screeners. However, staffing shortages and lack of high-speed connectivity at airport training facilities have made it difficult for screeners to fully utilize these programs. Specifically, TSA recently revamped its screener training program to include three main components: (1) training all screeners in the skills necessary for both passenger and baggage screening (replaces basic screener training); (2) recurrent (skills refresher) screener training; and (3) technical screener training/certification for EDS. In addition to strengthening its basic and recurrent training programs, TSA is enhancing and standardizing remedial training for screeners who fail testing conducted by TSA's Office of Internal Affairs and Program Review. TSA has also established leadership and technical training programs for screening supervisors.

Despite these efforts, however, some FSDs said that ensuring screeners received required training continued to be a challenge. For example, FSDs at 5 of the largest airports said that due to staffing shortages, they were unable to let screeners take training because it would impact FSDs' ability to provide adequate screener coverage. Consequently, screeners received an average of only 3 hours of recurrent training per month, far less than the required 3 hours per week.[9] In an attempt to ensure screeners receive required training, several FSDs provided training through overtime, or established training relief teams with the sole purpose of staffing screening checkpoints while screeners participated in training.

TSA Continues to Strengthen its Efforts to Measure Screener Performance in Detecting Threat Objects

TSA has undertaken several initiatives to measure the performance of passenger screeners in detecting threat objects. However, TSA has collected limited data related to the performance of baggage screeners. In July 2003, TSA completed a study of the performance of its passenger screening system, which identified numerous performance deficiencies, such as inadequate staffing and poor supervision of screeners. These deficiencies were in turn caused by a lack of skills and knowledge, low motivation, ineffective work environment, and wrong or missing incentives. In response to this study, in October 2003 TSA developed a short-term action plan that identified key actions TSA plans to take to strengthen the performance of passenger screeners. These actions built on

[9]TSA requires passenger and baggage screeners to participate in 3 hours of recurrent training per week, averaged over each quarter. One hour is required to be devoted to X-ray image interpretation, and the other 2 hours on screening techniques or reviews of standard operating procedures.

several initiatives that TSA already had underway, including enhancing training for screeners and supervisors, completing installation of the Threat Image Projection system,[10] and conducting annual recertifications of screeners. TSA is also increasing covert testing of passenger and baggage screeners in which TSA undercover agents attempt to pass threat objects through screening checkpoints to identify systematic problems affecting the performance of screeners.

While TSA is making progress in each of these areas, it has collected limited data on the performance of its baggage screening operations. Officials said that they have collected limited performance data related to baggage screeners due to their initial focus on passenger screener performance, but plan to collect additional performance data in the future.

TSA Faces Challenges in Its Efforts to Deploy and Leverage Screening Equipment and Technologies

TSA has made progress in its checked baggage screening operations, but continues to face operational and funding challenges in screening all checked baggage using explosive detection systems, as mandated by ATSA. Although TSA has deployed EDS and ETD equipment to all airports, TSA has not been able to fully utilize this equipment to screen 100 percent of checked baggage for explosives by the congressionally mandated deadline of December 31, 2003, due to screener and equipment shortages and equipment being out of service for maintenance and/or repairs. When TSA cannot screen 100 percent of checked baggage using EDS and ETD, TSA continues to use alternative means, including K-9 teams, manual bag searches, and positive passenger bag match. TSA has ongoing initiatives to increase the efficiency of screening checked baggage using EDS, including the development and construction of in-line baggage screening systems at larger airports—which streamlines the screening processes.

TSA is also conducting research and development activities to strengthen passenger and baggage screening. These efforts are designed to improve detection capability, performance, and efficiency for current technologies, and to develop the next generation of EDS equipment. However, progress on this research was delayed in fiscal year 2003 when TSA used $61 million of its $110 million research and development funds for other programs that TSA viewed as higher priorities. As a result, TSA had to delay several key research and development projects, including developing

[10]The Threat Image Projection system places images of threat objects on X-ray screens during actual screening operations and records whether screeners identify the objects.

a device to detect weapons, liquid explosives, and flammables in containers found in carry-on baggage or passengers' effects, and further development and testing of a walk-through chemical trace detection portal for detecting explosives on passengers.

Expansion of The Federal Air Marshal Service has experienced problems

Although measures are taken to keep dangerous individuals and items off aircraft, the possibility still exists that terrorists and dangerous objects can still get on board aircraft. Consequently, a number of other layers of security are in place to enhance the security of commercial aircraft while in transit. One such layer is the Federal Air Marshal Service, which places specially trained and armed teams of civil aviation security specialists on board aircraft to protect passengers, crew, and aircraft from terrorist activities on both domestic and international flights.

Following the September 11, 2001, terrorist attacks, the Service rapidly expanded. The organization grew from about 50 air marshals to 1,000s,[11] as the Deputy Secretary of the Department of Transportation—the Service's then parent agency—established a goal of hiring, training, and deploying the new air marshals by July 2002. The Service's budget grew commensurately, from $4.4 million in fiscal year 2001 to $545 million in fiscal year 2003. The rapid expansion led to a number of operational and management control issues for the Service. These included reviewing nearly 200,000 applications for federal air marshal positions, initiating thousands of background investigations for top-secret clearances, training the new workforce, and scheduling the air marshals for flight duty.

These operational and management control issues have caused a number of problems. As we discussed in a November 2003 report,[12] to deploy the requisite number of air marshals by July 2002, the Service revised and abbreviated its training program. It modified the air marshal training program from 14 weeks to about 5 weeks for candidates without prior law enforcement experience and to about 1 week for candidates with such experience. The training curriculum no longer included airplane cockpit familiarization, visits to airlines, and some of the instruction on the Service's policies and procedures. Moreover, air marshal candidates no

[11]The number of air marshals is classified.

[12]U.S. General Accounting Office, *Aviation Security: Federal Air Marshal Service Is Addressing Challenges of Its Expanded Mission and Workforce, but Additional Actions Needed*, GAO-04-242 (Washington, D.C.: Nov. 19, 2003).

longer had to pass an advanced marksmanship test to qualify for employment, although the candidates still had to pass a basic test. To provide the newly hired air marshals with the additional skills, the Service developed an advanced training course that the air marshals were required to complete by January 2004. However, cutbacks in funds have delayed the expected completion of this training by all air marshals until mid-2004.

Ongoing work that examines the funding of the Service indicates that problems may be continuing. Specifically, the number of air marshals has not reached established target levels and may be declining. The budget for the Service in fiscal year 2003—the year it was expected to achieve its target staffing level—was reduced by the department from $545 million to $450 million as part of a $763 million reprogramming by TSA to cover a number of funding shortfalls. As a result, the Service had to forgo the hiring of additional air marshals, further delay training, and reduce efforts to develop and equip much of its field operations infrastructure. The limitations on the funding for the Service, and on its ability to increase the number of air marshals to target levels, has resulted in the number of air marshals being less at the end of fiscal year 2003 than anticipated. Officials from the Service have said that if budget trends continue, they expect that at the end of fiscal year 2004 they will have fewer air marshals than they had at any point since mid-2002. Additionally, Service officials said that they do not have sufficient funding to develop the facilities needed to provide its field locations with key equipment and specialized space necessary for training and for providing updates on tactics and intelligence and to update the Service's automated mission scheduling system to enable it to schedule and manage all air marshal missions.

Concerns Exist in Other Aviation Security Areas

In addition to the concerns with the CAPPS II program, passenger and baggage screening, and the expansion of the Federal Air Marshal Service, TSA and DHS face a number of other programmatic and management concerns in strengthening aviation security. The concerns include developing measures to counter the Man-Portable Anti-aircraft Defense Systems (MANPADS) threat against commercial aircraft, implementing commercial airport perimeter and access controls, developing effective measures for ensuring the security of air cargo, and strengthening general aviation security. We have ongoing work that is examining DHS's and TSA's efforts in all of these areas.

MANPADS

The threat of terrorists using MANPADS—shoulder-launched surface-to-air missiles—against commercial aviation has increased in recent years, as many thousands of these missiles have been produced and are in national

arsenals and black markets throughout the world. In late 2002, terrorists fired surface-to-air missiles at an airliner departing from an airport in Kenya, marking the first time they had been used to attack commercial aircraft in a non-combat zone. Following the attack, the White House convened a task force to develop a strategy to reduce the MANPADS threat against commercial aircraft, and the Congress directed DHS to submit a plan to develop and demonstrate a counter-MANPADS device for commercial aircraft. In January 2004, DHS initiated a 2-year program to migrate existing military counter-MANPADS systems to the civil aviation environment and minimize the total lifecycle cost of such systems.

DHS faces significant challenges in adapting current military counter-MANPADS systems to commercial aircraft. These challenges include establishing system requirements, maturing the counter-MANPADS technology and design, and setting reliable cost estimates. For example, DHS has to account for a wide variety of aircraft types in designing and integrating the system. Further, the current generation of missile warning systems have high false alarm rates and high maintenance costs. In a January 2004 report,[13] we noted the benefits of following the knowledge-based approach used by leading developers in industry and government to reduce program risks and increase the likelihood of success and recommended that the department adopt this approach to develop a counter-MANPADS system for commercial aviation. DHS concurred with our recommendation and said that it will be using knowledge-based evaluations throughout the program.

We are continuing to examine U.S. efforts to control the international proliferation of MANPADS and DHS's efforts to develop technical countermeasures to minimize the threat of a MANPADS attack. We expect to issue a report discussing these issues by late April 2004.

Perimeter and Access Controls

Prior to September 2001, work performed by us and others highlighted the vulnerabilities in controls for limiting access to secure airport areas. In one report, we noted that our special agents were able to use fictitious law enforcement badges and credentials to gain access to secure areas, bypass

[13]U.S. General Accounting Office, *The Department of Homeland Security Needs to Fully Adopt a Knowledge-based Approach to Its Counter-MANPADS Development Program*, GAO-04-341R (Washington, D.C.: Jan. 30, 2004).

security checkpoints, and walk unescorted to aircraft departure gates.[14] The agents, who had been issued tickets and boarding passes, could have carried weapons, explosives, or other dangerous objects onto aircraft. Concerns over the adequacy of the vetting process for airport workers who have unescorted access to secure airport areas have also arisen, in part, as a result of federal agency airport security sweeps that uncovered hundreds of instances in which airport workers lied about their criminal history, or immigration status, or provided false or inaccurate Social Security numbers on their application for security clearances to obtain employment.

ATSA contains provisions to improve perimeter access security at the nation's airports and strengthen background checks for employees working in secure airport areas and TSA has made some progress in this area. For example, TSA issued several security directives to strengthen airport perimeter security by limiting the number of airport access points, and they require random screening of individuals, vehicles, and property before entry at the remaining perimeter access points. Further, TSA made criminal history checks mandatory for employees with access to secure or sterile airport areas. To date, TSA has conducted approximately 1 million of these checks. TSA plans to review security technologies in the areas of biometrics access control identification systems (i.e., fingerprints or iris scans), anti-piggybacking technologies (to prevent more than one employee from entering a secure area at a time), and video monitoring systems for perimeter security. Further, TSA plans to solicit commercial airport participation in a pilot airport security program and is currently reviewing information from interested airports. TSA plans to select 20 airports for the program.

Although progress has been made, challenges remain with perimeter security and access controls. Specifically, ATSA contains numerous requirements for strengthening perimeter security and access controls, some of which contained deadlines that TSA is working to meet. A number of technologies could be used to secure and monitor airport perimeters, including barriers, motion sensors, and closed-circuit television. Airport representatives have cautioned that as security enhancements are made to airport perimeters, it will be important for TSA to coordinate with the Federal Aviation Administration and the airport operators to ensure that

[14]U.S. General Accounting Office, *Security: Breaches at Federal Agencies and Airports*, GAO/T-OSI-00-10 (Washington, D.C.: May 25, 2000).

any enhancements do not pose safety risks for aircraft. To further examine these threats and challenges, we have ongoing work assessing TSA's progress in meeting ATSA provisions related to improving perimeter security, access controls, and background checks for airport employees and other individuals with access to secure areas of the airport, as well as the nature and extent of the threat from shoulder-fired missiles. We expect to report on the results of this work by May 2004.

Air Cargo Security

As we and the Department of Transportation's Inspector General have reported, vulnerabilities exist in ensuring the security of cargo carried aboard commercial passenger and all-cargo aircraft. The Federal Aviation Administration has reported that an estimated 12.5 million tons of cargo are transported each year—9.7 million tons on all-cargo planes and 2.8 million tons on passenger planes. Potential security risks are associated with the transport of air cargo—including the introduction of undetected explosive and incendiary devices in cargo placed aboard aircraft. To reduce these risks, ATSA requires that all cargo carried aboard commercial passenger aircraft be screened and that TSA have a system in place as soon as practicable to screen, inspect, or otherwise ensure the security of cargo on all-cargo aircraft. However, according to a September 2003 report by the Congressional Research Service, less than 5 percent of cargo placed on passenger airplanes is physically screened.[15] TSA's primary approach to ensuring air cargo security and safety is to ensure compliance with the "known shipper" program—which allows shippers that have established business histories with air carriers or freight forwarders to ship cargo on planes. However, we and the Department of Transportation's Inspector General have identified weaknesses in the known shipper program and in TSA's procedures for approving freight forwarders, such as possible tampering with freight at various handoff points before it is loaded into an aircraft.

Since September 2001, TSA has taken a number of actions to enhance cargo security, such as implementing a database of known shippers in October 2002. The database is the first phase in developing a cargo profiling system. However, in December 2002, we reported that additional operational and technological measures, such as checking the identity of individuals making cargo deliveries, had the potential to improve air cargo

[15]Congressional Research Service, *Air Cargo Security*, Sept. 11, 2003.

security in the near term.[16] We further reported that TSA lacks a comprehensive plan with long-term goals and performance targets for cargo security, time frames for completing security improvements, and risk-based criteria for prioritizing actions to achieve those goals. Accordingly, we recommended that TSA develop a comprehensive plan for air cargo security that incorporates a risk management approach, includes a list of security priorities, and sets deadlines for completing actions. TSA agreed with this recommendation and, in November 2003, issued its Air Cargo Strategic Plan. TSA also introduced a random inspection process for air cargo and outlined steps to strengthen the known shipper program. We will shortly begin a comprehensive review of air cargo security procedures, including these recent actions taken by TSA.

General Aviation Security

Not only are commercial aircraft a concern, but general aviation aircraft can be a security concern. TSA has taken limited action to improve general aviation security, leaving general aviation far more open and potentially vulnerable than commercial aviation. General aviation is vulnerable because general aviation pilots and passengers are not screened before takeoff and the contents of general aviation planes are not screened at any point. General aviation includes more than 200,000 privately owned airplanes, which are located in every state at more than 19,000 airports.[17] In the last 5 years, about 70 aircraft have been stolen from general aviation airports, indicating a potential weakness that could be exploited by terrorists. This vulnerability was demonstrated in January 2002, when a teenage flight student stole and crashed a single-engine airplane into a Tampa, Florida, skyscraper. Moreover, general aviation aircraft could be used in other types of terrorist acts. It was reported that the September 11th hijackers researched the use of crop dusters to spread biological or chemical agents.

We reported in September 2003 that TSA chartered a working group on general aviation within the existing Aviation Security Advisory Committee.[18] The working group consists of industry stakeholders and is

[16]U.S. General Accounting Office, *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System*, GAO-03-344 (Washington, D.C.: Dec. 20, 2002).

[17]Of the 19,000 general aviation airports, 5,400 are publicly owned. TSA is currently focusing its efforts on these publicly owned airports.

[18]U.S. General Accounting Office, *Aviation Security: Progress since September 11th, and the Challenges Ahead*, GAO-03-1150T (Washington, D.C.: Sept. 9, 2003).

designed to identify and recommend actions to close potential security gaps in general aviation. On October 1, 2003, the working group issued a report that included a number of recommendations for general aviation airport operators' voluntary use in evaluating airports' security requirements. These recommendations are both broad in scope and generic in their application, with the intent that every general aviation airport and landing facility operators may use them to evaluate that facility's physical security, procedures, infrastructure, and resources. TSA will use these recommendations as a baseline to develop a set of federally endorsed guidelines for enhancing airport security at general aviation facilities throughout the nation. TSA is taking some additional action to strengthen security at general aviation airports, including developing a risk-based self-assessment tool for general aviation airports to use in identifying security concerns. We have ongoing work that is examining general aviation security in further detail; we expect to report on this work in the fall of 2004.

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

Contact Information

For further information on this testimony, please contact Norman J. Rabkin at (202) 512-8777. Individuals making key contributions to this testimony include J. Michael Bollinger, Adam Hoffman, and John R. Schulze.

Appendix: Related GAO Products

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

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

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

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

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

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

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

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

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

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

Aviation Security: Measures Needed to Improve Security of Pilot Certification Process. GAO-03-248NI. Washington, D.C.: February 3, 2003. (NOT FOR PUBLIC DISSEMINATION).

Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System. GAO-03-286NI. Washington, D.C.: December 20, 2002. (NOT FOR PUBLIC DISSEMINATION).

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

Aviation Security: Vulnerability of Commercial Aviation to Attacks by Terrorists Using Dangerous Goods. GAO-03-30C. Washington, D.C.: December 3, 2002.

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

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

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

Aviation Security: Deployment and Capabilities of Explosive Detection Equipment. GAO-02-713C. Washington, D.C.: June 20, 2002. (CLASSIFIED).

Aviation Security: Information on Vulnerabilities in the Nation's Air Transportation System. GAO-01-1164T. Washington, D.C.: September 26, 2001. (NOT FOR PUBLIC DISSEMINATION).

Aviation Security: Information on the Nation's Air Transportation System Vulnerabilities. GAO-01-1174T. Washington, D.C.: September 26, 2001. (NOT FOR PUBLIC DISSEMINATION).

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

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

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

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

Responses of Federal Agencies and Airports We Surveyed about Access Security Improvements. GAO-01-1069R. Washington, D.C.: August 31, 2001.

Responses of Federal Agencies and Airports We Surveyed about Access Security Improvements. GAO-01-1068R. Washington, D.C.: August 31, 2001. (RESTRICTED).

FAA Computer Security: Recommendations to Address Continuing Weaknesses. GAO-01-171. Washington, D.C.: December 6, 2000.

Aviation Security: Additional Controls Needed to Address Weaknesses in Carriage of Weapons Regulations. GAO/RCED-00-181. Washington, D.C.: September 29, 2000.

FAA Computer Security: Actions Needed to Address Critical Weaknesses That Jeopardize Aviation Operations. GAO/T-AIMD-00-330. Washington, D.C.: September 27, 2000.

FAA Computer Security: Concerns Remain Due to Personnel and Other Continuing Weaknesses. GAO/AIMD-00-252. Washington, D.C.: August 16, 2000.

Aviation Security: Long-Standing Problems Impair Airport Screeners' Performance. GAO/RCED-00-75. Washington, D.C.: June 28, 2000.

Aviation Security: Screeners Continue to Have Serious Problems Detecting Dangerous Objects. GAO/RCED-00-159. Washington, D.C.: June 22, 2000. (NOT FOR PUBLIC DISSEMINATION).

Security: Breaches at Federal Agencies and Airports. GAO/T-OSI-00-10. Washington, D.C.: May 25, 2000.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

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

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Public Affairs

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