United States General Accounting Office

GAO

Testimony

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

For Release on Delivery
Expected at
9:30 a.m. EDT
Tuesday
September 9, 2003

AVIATION SECURITY

Progress Since September 11, 2001, and the Challenges Ahead

Statement of Gerald L. Dillingham,
Director, Civil Aviation Issues

GAO-03-1150T

September 9, 2003

AVIATION SECURITY

Progress Since September 11, 2001, and the Challenges Ahead

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-1150T, a testimony before the Committee on Commerce, Science and Transportation, U.S. Senate

Why GAO Did This Study

In the 2 years since the terrorist attacks of September 11, 2001, the security of our nation's civil aviation system has assumed renewed urgency, and efforts to strengthen aviation security have received a great deal of congressional attention. On November 19, 2001, the Congress enacted the Aviation and Transportation Security Act (ATSA), which created the Transportation Security Administration (TSA) within the Department of Transportation (DOT) and defined its primary responsibility as ensuring security in aviation as well as in other modes of transportation. The Homeland Security Act, passed on November 25, 2002, transferred TSA to the new Department of Homeland Security, which assumed overall responsibility for aviation security. GAO was asked to describe the progress that has been made since September 11 to strengthen aviation security, the potential vulnerabilities that remain, and the longer-term management and organizational challenges to sustaining enhanced aviation security.

What GAO Recommends

In prior reports and testimonies, listed at the end of this statement, GAO has made numerous recommendations to strengthen aviation security and to improve the management of federal aviation security organizations and functions.

www.gao.gov/cgi-bin/getrpt?GAO-03-1150T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gerald L. Dillingham, Ph.D., at (202) 512-2834 or dillinghamg@gao.gov.

What GAO Found

Since September 11, 2001, TSA has made considerable progress in meeting congressional mandates designed to increase aviation security. By the end of 2002, the agency had hired and deployed about 65,000 passenger and baggage screeners, federal air marshals, and others, and it was using explosives detection equipment to screen about 90 percent of all checked baggage. TSA is also initiating or developing efforts that focus on the use of technology and information to advance security. One effort under development, the next-generation Computer-Assisted Passenger Prescreening System (CAPPS II), would use national security and commercial databases to identify passengers who could pose risks for additional screening. Concerns about privacy rights will need to be addressed as this system moves toward implementation.

Although TSA has focused on ensuring that bombs and other threat items are not carried onto planes by passengers or in their luggage, vulnerabilities remain in air cargo, general aviation, and airport perimeter security. Each year, an estimated 12.5 million tons of cargo are transported on all-cargo and passenger planes, yet very little air cargo is screened for explosives. We have previously recommended, and the industry has suggested, that TSA use a risk-management approach to set priorities as it works with the industry to determine the next steps in strengthening aviation security.

TSA faces longer-term management and organizational challenges to sustaining enhanced aviation security that include (1) developing and implementing a comprehensive risk management approach, (2) paying for increased aviation security needs and controlling costs, (3) establishing effective coordination among the many entities involved in aviation security, (4) strategically managing its workforce, and (5) building a results-oriented culture within the new Department of Homeland Security. TSA has begun to respond to recommendations we have made addressing many of these challenges, and we have other studies in progress.

Air Cargo Remains Vulnerable to Terrorist Threats

Mr. Chairman and Members of the Committee:

In the 2 years since the terrorist attacks of September 11, 2001, the security of our nation's civil aviation system has assumed renewed urgency, and efforts to strengthen aviation security have received a great deal of congressional attention. On November 19, 2001, the Congress enacted the Aviation and Transportation Security Act (ATSA), which created the Transportation Security Administration (TSA) within the Department of Transportation (DOT) and defined its primary responsibility as ensuring security in aviation as well as in other modes of transportation. The act set forth specific improvements to aviation security for TSA to implement and established deadlines for completing many of them. The Homeland Security Act, passed on November 25, 2002, transferred TSA to the new Department of Homeland Security, which assumed overall responsibility for aviation security.

My testimony today addresses the (1) progress that has been made since September 11 to strengthen aviation security, (2) potential vulnerabilities that remain, and (3) longer-term management and organizational challenges to sustaining enhanced aviation security. The testimony is based on our prior work, our review of recent literature, and discussions with aviation industry representatives and TSA.

In summary:

Since September 2001, TSA has made considerable progress in meeting congressional mandates related to aviation security, thereby increasing aviation security. For example, by the end of December 2002, the agency had hired and deployed a workforce of about 65,000, including passenger and baggage screeners and federal air marshals, and it was using explosives detection equipment to screen about 90 percent of all checked baggage. In addition, TSA has initiated several programs and research and development efforts that focus on the use of technology and information to advance security. For example, the agency is developing the Transportation Workers Identification Card program to provide a nationwide standard credential for airport workers that is issued after a background check has been completed and biometric indicators have been incorporated so that each worker can be positively matched to his or her credential. TSA is also developing the next-generation Computer Assisted Passenger Prescreening System (CAPPS II), which would use national security and commercial databases to assess the risk posed by passengers and identify some passengers for additional screening before they board their flights. These uses of technology and information—particularly

CAPPS II—have raised some concerns about privacy rights that will need to be addressed as these programs move toward implementation.

Although TSA has focused much effort and funding on ensuring that bombs and other threat items are not carried onto planes by passengers or in their luggage, vulnerabilities remain in areas such as air cargo security, general aviation security, and airport perimeter security. For example, air cargo is vulnerable because very little of the estimated 12.5 million tons transported each year on all-cargo and passenger planes is physically screened for explosives. As a result, a potential security risk is the introduction of explosive and incendiary devices in cargo placed aboard aircraft. We have recommended in prior work that TSA use a risk management approach to prioritize actions and funding as it works with industry to determine the next steps in strengthening air cargo security, and industry stakeholders have suggested the application of such an approach to general aviation security.

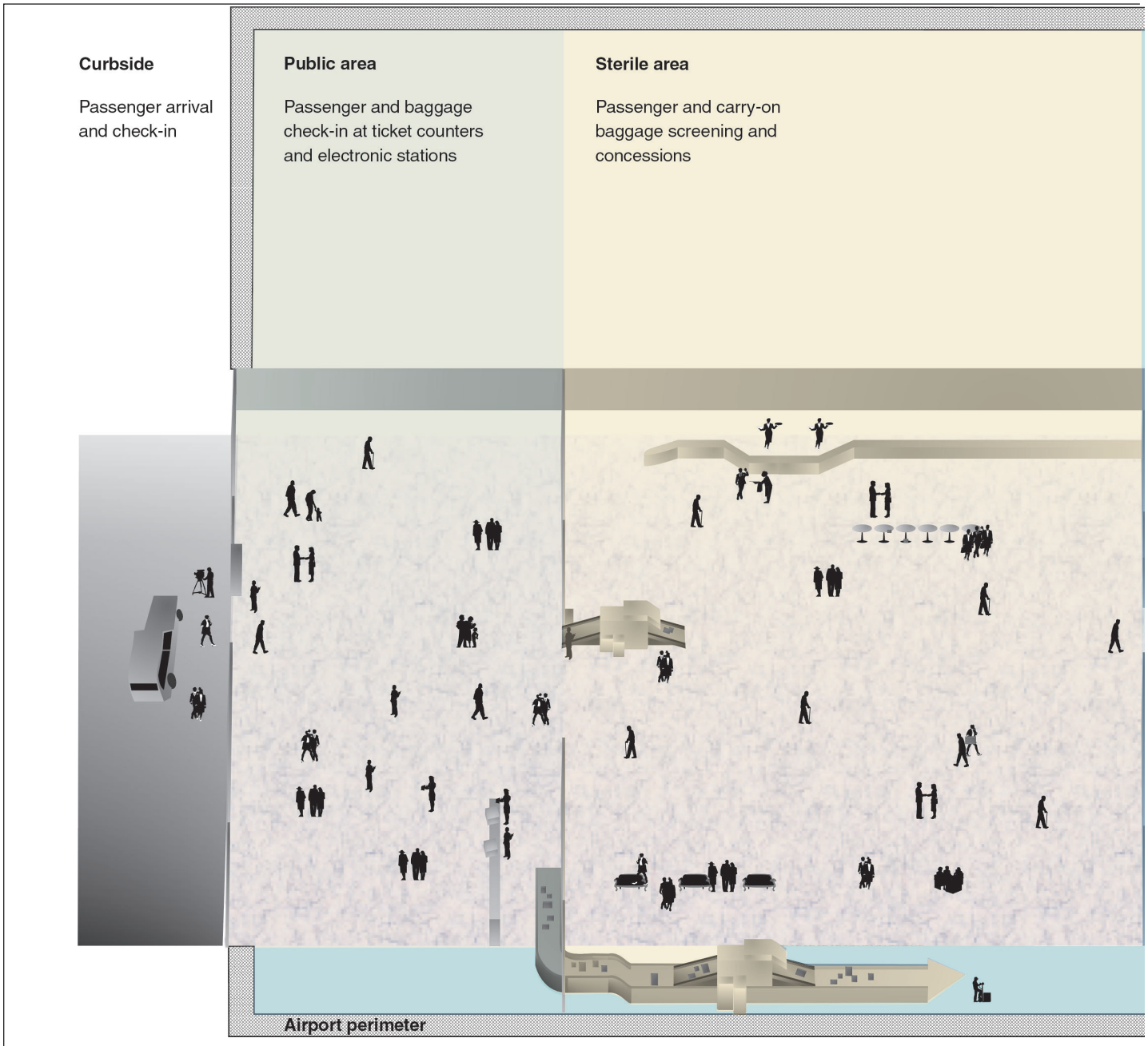
TSA faces longer-term management and organizational challenges to sustaining enhanced aviation security that include (1) developing and implementing a comprehensive risk management approach, (2) paying for increased aviation security needs and controlling costs, (3) establishing effective coordination among the many public and private entities involved in aviation security, (4) strategically managing its workforce and ensuring appropriate staffing levels, and (5) building a results-oriented culture as it shifts its aviation security and other functions to the Department of Homeland Security. We have issued reports and made recommendations that address many of these challenges, and some actions are under way. In addition, we have studies in progress on some of these issues.

Background

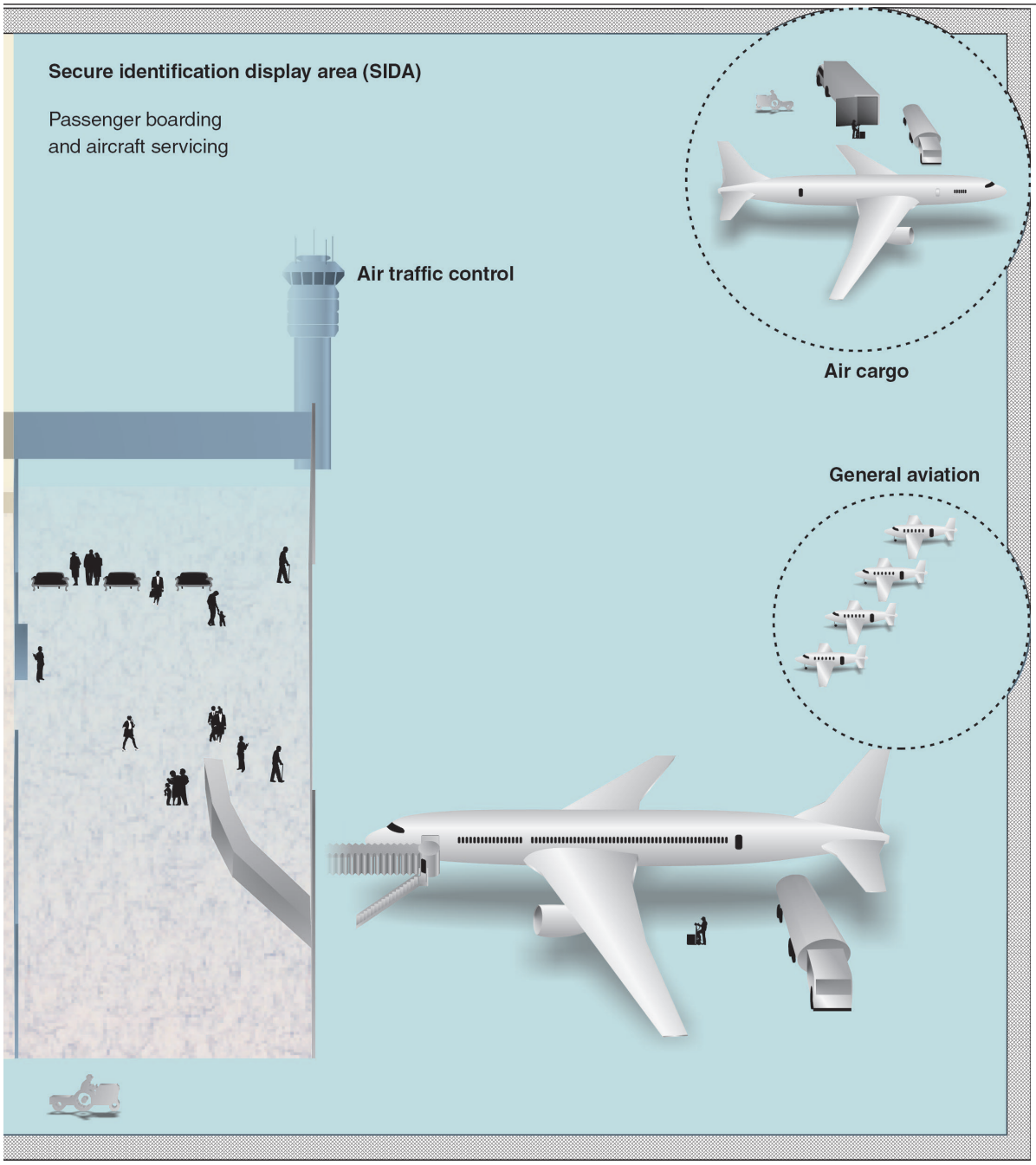
Before September 2001, we and others had demonstrated significant, long-standing vulnerabilities in aviation security, some of which are depicted in figure 1. These included weaknesses in screening passengers and baggage, controlling access to secure areas at airports, and protecting air traffic control computer systems and facilities. To address these and other weaknesses, ATSA created the Transportation Security Administration and established security requirements for the new agency with mandated deadlines.

This page intentially left blank

Figure 1: Aviation Security Focus Areas



Source: GAO.


Secure identification display area (SIDA)
Passenger boarding
and aircraft servicing
Air traffic control
Air cargo
General aviation

Civil Aviation Was Vulnerable before September 11, 2001

Before September 2001, screeners, who were then hired by the airlines, often failed to detect threat objects located on passengers or in their carry-on luggage. Principal causes of screeners' performance problems were rapid turnover and insufficient training. As we previously reported, turnover rates exceeded 100 percent a year at most large airports, leaving few skilled and experienced screeners, primarily because of low wages, limited benefits, and repetitive, monotonous work.[1]

In addition, before September 2001, controls for limiting access to secure areas of airports, including aircraft, did not always work as intended. As we reported in May 2000, our special agents used fictitious law enforcement badges and credentials to gain access to secure areas, bypass security checkpoints at two airports, and walk unescorted to aircraft departure gates.[2] The agents, who had been issued tickets and boarding passes, could have carried weapons, explosives, or other dangerous objects onto aircraft. DOT's Inspector General also documented numerous problems with airport access controls, and in one series of tests, nearly 7 out of every 10 attempts by the Inspector General's staff to gain access to secure areas were successful. Upon entering the secure areas, the Inspector General's staff boarded aircraft 117 times. The Inspector General further reported that the majority of the aircraft boardings would not have occurred if employees had taken the prescribed steps, such as making sure doors closed behind them.

Our reviews also found that the security of the air traffic control computer systems and of the facilities that house them had not been ensured.[3] The vulnerabilities we identified, such as not ensuring that contractors who

[1]U.S. General Accounting Office, *Aviation Security: Long-Standing Problems Impair Airport Screeners' Performance*, GAO/RCED-00-75 (Washington, D.C.: June 28, 2000) and U.S. General Accounting Office, *Aviation Security: Terrorist Acts Illustrate Severe Weaknesses in Aviation Security*, GAO-01-1166T (Washington, D.C.: Sept. 20, 2001).

[2]U.S. General Accounting Office, *Security: Breaches at Federal Agencies and Airports*, GAO-OSI-0010 (Washington, D.C.: May 25, 2000).

[3]U.S. General Accounting Office, *Aviation Security: Weak Computer Security Practices Jeopardize Flight Safety*, GAO/AIMD-98-155 (Washington, D.C.: May 18, 1998); *Computer Security: FAA Needs to Improve Controls over Use of Foreign Nationals to Remediate and Review Software*, GAO/AIMD-00-55 (Washington, D.C.: Dec. 23, 1999); *Computer Security: FAA Is Addressing Personnel Weaknesses, but Further Action Is Required*, GAO/AIMD-00-169 (Washington, D.C.: May 31, 2000); *FAA Computer Security: Concerns Remain Due to Personnel and Other Continuing Weaknesses*, GAO/AIMD-00-252 (Washington, D.C.: Aug. 16, 2000); and *FAA Computer Security: Recommendations to Address Continuing Weaknesses*, GAO-01-171 (Washington, D.C.: Dec. 6, 2000).

had access to the air traffic control computer systems had undergone background checks, made the air traffic control system susceptible to intrusion and malicious attacks. The air traffic control computer systems provide information to air traffic controllers and aircraft flight crews to help ensure the safe and expeditious movement of aircraft. Failure to protect these systems and their facilities could cause a nationwide disruption of air traffic or even collisions and loss of life.

Over the years, we made numerous recommendations to the Federal Aviation Administration (FAA), which, until ATSA's enactment, was responsible for aviation security. These recommendations were designed to improve screeners' performance, strengthen airport access controls, and better protect air traffic control computer systems and facilities. As of September 2001, FAA had implemented some of these recommendations and was addressing others, but its progress was often slow. In addition, many initiatives were not linked to specific deadlines, making it difficult to monitor and oversee their implementation.

Legislation Transferred Most Aviation Security Responsibilities to TSA

ATSA defined TSA's primary responsibility as ensuring security in all modes of transportation. The act also shifted security-screening responsibilities from the airlines to TSA and established a series of requirements to strengthen aviation security, many of them with mandated implementation deadlines. For example, the act required the deployment of federal screeners at 429 commercial airports across the nation by November 19, 2002, and the use of explosives detection technology at these airports to screen every piece of checked baggage for explosives not later than December 31, 2002. However, the Homeland Security Act subsequently allowed TSA to grant waivers of up to 1 year to airports that would not be able to meet the December deadline.

Some aviation security responsibilities remained with FAA. For example, FAA is responsible for the security of its air traffic control and other computer systems and of its air traffic control facilities. FAA also administers the Airport Improvement Program (AIP) trust fund, which is used to fund capital improvements to airports, including some security enhancements, such as terminal modifications to accommodate explosives detection equipment.

Since September 2001, Multiple Initiatives Have Increased Aviation Security

Over the past 2 years, TSA and FAA have taken major steps to increase aviation security. TSA has implemented congressional mandates and explored options for increasing the use of technology and information to control access to secure areas of airports and to improve passenger screening. FAA has focused its efforts on enhancing the security of the nation's air traffic control systems and facilities. In ongoing work, we are examining some of these efforts in more detail (see app. IV).

TSA Met Many Aviation Security Mandates but Encountered Some Difficulties

In its first year, TSA worked to establish its organization and focused primarily on meeting the aviation security deadlines set forth in ATSA, accomplishing a large number of tasks under a very ambitious schedule. In January 2002, TSA had 13 employees—1 year later, the agency had about 65,000 employees. TSA reported that it met over 30 deadlines during 2002 to improve aviation security. (See app. I for the status of mandates in ATSA.) For example, according to TSA, it

- met the November 2002 deadline to deploy federal passenger screeners at airports across the nation by hiring, training, and deploying over 40,000 individuals to screen passengers at 429 commercial airports (see fig. 2);
- hired and deployed more than 20,000 individuals to screen all checked baggage;
- has been using explosives detection systems or explosives trace detection equipment to screen about 90 percent of all checked baggage as of December 31, 2002;[4]
- has been using alternative means such as canine teams, hand searches, and passenger-bag matching to screen the remaining checked baggage;
- confiscated more than 4.8 million prohibited items (including firearms, knives, and incendiary or flammable objects) from passengers; and
- has made substantial progress in expanding the Federal Air Marshal Service.

[4]Explosives detection machines are used to screen baggage for explosives and work by using CAT scan X-ray technology to take fundamental measurements of materials in bags to recognize characteristic signatures of threat explosives. Explosives trace detection systems (trace detection machines) are used to screen baggage for explosives, and work by detecting vapors and residues of explosives.

In addition, according to FAA, U.S. and foreign airlines met the April 2003 deadline to harden cockpit doors on aircraft flying in the United States.

Figure 2: Screening Passengers at a U.S. Commercial Airport

Source: FAA.

Not unexpectedly, TSA experienced some difficulties in meeting these deadlines and achieving these goals. For example, operational and management control problems, cited later in this testimony, emerged with the rapid expansion of the Federal Air Marshal Service, and TSA's deployment of some explosives detection systems was delayed. As a

result, TSA had to grant waivers of up to a year (until Dec. 31, 2003) to a few airports, authorizing them to use alternative means to screen all checked baggage. Recently, airport representatives with whom we spoke expressed concern that not all of these airports would meet the new December 2003 deadline established in their waivers because, according to the airport representatives, there has not been enough time to produce, install, and integrate all of the systems required to meet the deadline.

TSA Is Making Greater Use of Technology and Information to Enhance Aviation Security

To strengthen control over access to secure areas of airports and other transportation facilities, TSA is pursuing initiatives that make greater use of technology and information. For example, the agency is investigating the establishment of a Transportation Workers Identification Card (TWIC) program. TWIC is intended to establish a uniform, nationwide standard for the secure identification of 12 million workers who require unescorted physical or cyber access to secure areas at airports and other transportation facilities. Specifically, TWIC will combine standard background checks and biometrics so that a worker can be positively matched to his or her credential. Once the program is fully operational, the TWIC card will be the standard credential for airport workers and will be accepted by all modes of transportation. According to TSA, developing a uniform, nationwide standard for identification will minimize redundant credentialing and background checks. Currently, each airport is required, as part of its security program, to issue credentials to workers who need access to secure, nonpublic areas, such as baggage loading areas.[5] Airport representatives have told us that they think a number of operational issues need to be resolved for the TWIC card to be feasible. For example, the TWIC card would have to be compatible with the many types of card readers used at airports around the country, or new card readers would have to be installed. At large airports, this could entail replacing hundreds of card readers, and airport representatives have expressed concerns about how this effort would be funded. In April 2003, TSA awarded a contract to test and evaluate various technologies at three pilot sites.

In addition, TSA has continued to develop the next-generation Computer Assisted Passenger Prescreening System (CAPPS II)—an automated passenger screening system that takes personal information, such as a

[5]Under 49 C.F.R. sec. 1542.101, all qualified airports are required to have a TSA-approved security program that includes procedures to control movement within the secured area, including identification media required under sec. 1542.201(b)(3).

passenger's name, date of birth, home address, and home telephone number, to confirm the passenger's identity and assess a risk level. The identifying information will be run against national security information and commercial databases, and a "risk" score will be assigned to the passenger. The risk score will determine any further screening that the passenger will undergo before boarding. TSA expects to implement CAPPS II throughout the United States by the fall of 2004. However, TSA's plans have raised concerns about travelers' privacy rights. It has been suggested, for example, that TSA is violating privacy laws by not explaining how the risk assessment data will be scored and used and how a TSA decision can be appealed. These concerns about the system will need to be addressed as it moves toward implementation. In ongoing work, we are examining CAPPS II, including how it will function, what safeguards will be put in place to protect the traveling public's privacy, and how the system will affect the traveling public in terms of costs, delays, and risks.

Additionally, TSA has begun to develop initiatives that could enable it to use its passenger screening resources more efficiently. For example, TSA has requested funding for fiscal year 2004 to begin developing a registered traveler program that would prescreen low-risk travelers. Under a registered traveler program, those who voluntarily apply to participate in the program and successfully pass background checks would receive a unique identifier or card that would enable them to be screened more quickly and would promote greater focus on those passengers who require more extensive screening at airport security checkpoints. In prior work, we identified key policy and implementation issues that would need to be resolved before a registered traveler program could be implemented. Such issues include the (1) criteria that should be established to determine eligibility to apply for the program, (2) kinds of background checks that should be used to certify applicants' eligibility to enroll in the program and the entity who should perform these checks, (3) security-screening procedures that registered travelers should undergo and the differences between these procedures and those for unregistered travelers, and (4) concerns that the traveling public or others may have about equity, privacy, and liability.[6]

[6]U.S. General Accounting Office, *Aviation Security: Registered Traveler Program Policy and Implementation Issues*, GAO-03-253 (Washington, D.C.: Nov. 22, 2002).

FAA Is Strengthening Air Traffic Control Security

Since September 2001, FAA has continued to strengthen the security of the nation's air traffic control computer systems and facilities in response to 39 recommendations we made between May 1998 and December 2000. For example, FAA has established an information systems security management structure under its Chief Information Officer, whose office has developed an information systems security strategy, security architecture (that is, an overall blueprint), security policies and directives, and a security awareness training campaign. This office has also managed FAA's incident response center and implemented a certification and accreditation process to ensure that vulnerabilities in current and future air traffic control systems are identified and weaknesses addressed. Nevertheless, the office faces continued challenges in increasing its intrusion detection capabilities, obtaining accreditation for systems that are already operational, and managing information systems security throughout the agency. In addition, according to senior security officials, FAA has completed assessments of the physical security of its staffed facilities, but it has not yet accredited all of these air traffic control facilities as secure in compliance with its own policy. Finally, FAA has worked aggressively over the past 2 years to complete background investigations of numerous contractor employees. However, ensuring that all new contractors are assessed to determine which employees require background checks, and that those checks are completed in a timely manner, will be a continuing challenge for the agency.

Potential Vulnerabilities Remain in Several Aviation Sectors

Although TSA has focused much effort and funding on ensuring that bombs and other threat items are not carried onto commercial aircraft by passengers or in their luggage, vulnerabilities remain, according to aviation experts, TSA officials, and others. In particular, these vulnerabilities affect air cargo, general aviation, and airport perimeter security. For information on legislative proposals that would address these potential vulnerabilities and other aviation security issues, see appendix II.

Air Cargo Security

As we and DOT's Inspector General have reported, vulnerabilities exist in securing the cargo carried aboard commercial passenger and all-cargo aircraft. TSA 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. Some potential security risks associated with air cargo include the introduction of undetected explosive and incendiary

devices in cargo placed aboard aircraft; the shipment of undeclared or undetected hazardous materials aboard aircraft; and aircraft hijackings and sabotage by individuals with access to cargo aircraft.[7] To address some of the risks associated with air cargo, 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. In August 2003, the Congressional Research Service reported that less than 5 percent of cargo placed on passenger airplanes is physically screened. TSA's primary approach to ensuring air cargo security and safety and to complying with the cargo-screening requirement in the act is the "known shipper" program—which allows shippers that have established business histories with air carriers or freight forwarders[8] to ship cargo on planes. However, we and DOT's Inspector General have identified weaknesses in the known shipper program and in TSA's procedures for approving freight forwarders.[9]

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 similar to the Computer-Assisted Passenger Prescreening System. However, in December 2002, we reported that additional operational and technological measures, such as checking the identity of individuals making cargo deliveries, have the potential to improve air cargo security in the near term.[10] 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

[7]For example, on November 15, 1979, an explosive device contained in a parcel shipped by U.S. mail exploded aboard an American Airlines flight; on April 7, 1994, a Federal Express employee attempted to hijack a company plane and crash it into the company's headquarters. We reported on the security risks associated with dangerous goods in *Aviation Security: Vulnerability of Commercial Aviation to Attacks by Terrorists Using Dangerous Goods*, GAO-03-30C (Washington, D.C.: Dec. 3, 2002).

[8]Freight forwarders consolidate shipments and deliver them to air carriers and cargo facilities of passenger and all-cargo air carriers.

[9]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).

[10]GAO-03-344.

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 expects to develop such a plan by the fall of 2003. It will be important that this plan include a timetable for implementation and that TSA expeditiously reduce the vulnerabilities in this area.

General Aviation Security

Since September 2001, TSA has taken limited action to improve general aviation security, leaving it far more open and potentially vulnerable than commercial aviation.[11] General aviation is vulnerable because general aviation pilots 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. Over 550 of these airports also provide commercial service. 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. Moreover, it was reported that the September 11 hijackers researched the use of crop dusters to spread biological or chemical agents. General aviation's vulnerability was revealed in January 2002, when a Florida teenage flight student crashed a single-engine Cessna airplane into a Tampa skyscraper.

FAA has since issued a notice with voluntary guidance for flight schools and businesses that provide services for aircraft and pilots at general aviation airports. The suggestions include using different keys to gain access to an aircraft and start the ignition, not giving students access to aircraft keys, ensuring positive identification of flight students, and training employees and pilots to report suspicious activities. However, because the guidance is voluntary, it is unknown how many general aviation airports have implemented these measures.

We reported in June 2003 that TSA was working with industry stakeholders as part of TSA's Aviation Security Advisory Council to close potential security gaps in general aviation.[12] According to our recent

[11]For example, TSA issued a rule requiring that certain aircraft operators using aircraft with a maximum takeoff weight of 12,500 pounds or more carry out security measures, including conducting criminal history records checks on their flight crew members and restricting access to the flight deck. This rule went into effect in April 2003.

[12]U.S. General Accounting Office, *Transportation Security: Federal Action Needed to Help Address Security Challenges*, GAO-03-843 (Washington, D.C.: June 30, 2003).

discussions with industry representatives, however, the stakeholders have not been able to reach a consensus on the actions needed to improve security in general aviation. General aviation industry representatives, such as the Aircraft Owners and Pilots Association and General Aviation Manufacturers Association, have opposed any restrictions on operating general aviation aircraft and believe that small planes do not pose a significant risk to the country. Nonetheless, some industry representatives indicated that the application of a risk management approach would be helpful in determining the next steps in improving general aviation security. (We discuss risk management in more detail later in this testimony.) To identify these next steps, TSA chartered a working group on general aviation within the existing Aviation Security Advisory Committee, and this working group is scheduled to report to the full committee in the fall of 2003. We have ongoing work that is examining general aviation security in further detail.

Figure 3: General Aviation Aircraft and Airport

Source: Aircraft Owners and Pilots Association.

Airport Perimeter Security

Airport perimeters present a potential vulnerability by providing a route for individuals to gain unauthorized access to aircraft and secure areas of airports (see fig. 4). For example, in August 2003, the national media reported that three boaters wandered the tarmac at Kennedy International Airport after their boat became beached near a runway. In addition, terrorists could launch an attack using a shoulder-fired missile from the perimeter of an airport, as well as from locations just outside the perimeter. For example, in separate incidents in the late 1970s, guerrillas with shoulder-fired missiles shot down two Air Rhodesia planes. More recently, the national media have reported that since September 2001, al

Qaeda has twice tried to down planes outside the United States with shoulder-fired missiles.[13]

We reported in June 2003 that airport operators have increased their patrols of airport perimeters since September 2001, but industry officials stated that they do not have enough resources to completely protect against missile attacks.[14] 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 FAA and the airport operators to ensure that any enhancements do not pose safety risks for aircraft. We have separate ongoing work examining the status of efforts to improve airport perimeter security and assessing the nature and extent of the threat from shoulder-fired missiles.

[13]The Department of Homeland Security is assessing proposals from eight contractors for technology to protect commercial aircraft from shoulder-fired missile attack.

[14]GAO-03-843.

Figure 4: Airport Perimeter

Source: GAO.

Aviation Security Poses Longer-Term Management and Organizational Challenges

TSA's efforts to strengthen and sustain aviation security face several longer-term challenges in the areas of risk management, funding, coordination, strategic human capital management, and building a results-oriented organization.

Risk Management

As aviation security is viewed in the larger context of transportation and homeland security, it will be important to set strategic priorities so that national resources can be directed to the greatest needs. Although TSA initially focused on increasing aviation security, it has more recently begun to address security in the other transportation modes. However, the size and diversity of the national transportation system make it difficult to adequately secure, and TSA and the Congress are faced with demands for additional federal funding for transportation security that far exceed the additional amounts made available. We have advocated the use of a risk management approach to guide federal programs and responses to better prepare for and withstand terrorist threats, and we have recommended that TSA use this approach to strengthen security in aviation as well as in other transportation modes.[15] A risk management approach is a systematic process to analyze threats, vulnerabilities, and the criticality (or relative importance) of assets to better support key decisions linking resources with prioritized efforts for results. Comprehensive risk-based assessments support effective planning and resource allocation. Figure 5 describes this approach.

Figure 5: Elements of a Risk Management Approach

A threat assessment identifies and evaluates potential threats on the basis of factors such as capabilities, intentions, and past activities. This assessment represents a systematic approach to identifying potential threats before they materialize. However, even if updated often, a threat assessment might not adequately capture some emerging threats. The risk management approach, therefore, uses vulnerability and criticality assessments as additional input to the decisionmaking process.

A vulnerability assessment identifies weaknesses that may be exploited by identified threats and suggests options to address those weaknesses.

A criticality assessment evaluates and prioritizes assets and functions in terms of specific criteria, such as their importance to public safety and the economy. The assessment provides a basis for identifying which structures or processes are relatively more important to protect from attack. As such, it helps managers to determine operational requirements and target resources at the highest priorities, while reducing the potential for targeting resources at lower priorities.

Source: GAO.

[15]U.S. General Accounting Office, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Washington, D.C.: Oct. 31, 2001); and GAO-03-344.

TSA agreed with our recommendation and has adopted a risk management approach in attempting to enhance security across all transportation modes. TSA's Office of Threat Assessment and Risk Management is developing two assessment tools that will help assess criticality, threats, and vulnerabilities. The first tool, which assesses criticality, will arrive at a criticality score for a facility or transportation asset by incorporating factors such as the number of fatalities that could occur during an attack and the economic and sociopolitical importance of the facility or asset. This score will enable TSA, in conjunction with transportation stakeholders, to rank facilities and assets within each mode and thus focus resources on those that are deemed most important. TSA is working with another Department of Homeland Security office—the Information Analysis and Infrastructure Protection Directorate—to ensure that the criticality tool will be consistent with the Department's overall approach for managing critical infrastructure.

The second tool—the Transportation Risk Assessment and Vulnerability Evaluation tool (TRAVEL)—will assess threats and analyze vulnerabilities for all transportation modes. The tool produces a relative risk score for potential attacks against a transportation asset or facility. In addition, TRAVEL will include a cost-benefit component that compares the cost of implementing a given countermeasure with the reduction in relative risk due to that countermeasure. We reported in June 2003 that TSA plans to use this tool to gather comparable threat and vulnerability information across all transportation modes. It is important for TSA to complete the development of the two tools and use them to prepare action plans for specific modes, such as aviation, and for transportation security generally.

Funding

Two key funding and accountability challenges will be (1) paying for increased aviation security and (2) ensuring that these costs are controlled. The costs associated with the equipment and personnel needed to screen passengers and their baggage alone are huge. The administration requested $4.2 billion for aviation security for fiscal year 2004, which included about $1.8 billion for passenger screening and $944 million for baggage screening.[16] ATSA created a passenger security fee to pay for the costs of aviation security, but the fee has not generated enough money to

[16]The House agreed to $3.7 billion in funding for TSA and the Senate approved $4.5 billion.

do so. DOT's Inspector General reported that the security fees are estimated to generate only about $1.7 billion in fiscal year 2004.[17]

A major funding issue is paying for the purchase and installation of the remaining explosives detection systems for the airports that received waivers, as well as for the reinstallation of the systems that were placed in airport lobbies last year and now need to be integrated into airport baggage-handling systems. Integrating the equipment with the baggage-handling systems is expected to be costly because it will require major facility modifications. For example, modifications needed to integrate the equipment at Boston's Logan International Airport are estimated to cost $146 million. Estimates for Dallas/Fort Worth International Airport are $193 million. DOT's Inspector General has reported that the cost of integrating the equipment nationwide could be as high as $3 billion.

A key question is how to pay for these installation costs. Funds from FAA's AIP grants and passenger facility charges are eligible sources for funding this work.[18] In fiscal year 2002, AIP grant funds totaling $561 million were used for terminal modifications to enhance security. However, using these funds for security reduced the funding available for other airport development projects, such as projects to bring airports up to federal design standards and reconstruction projects. In February 2003, we identified letters of intent[19] as a funding option that has been successfully used to leverage private sources of funding.[20] TSA has since signed letters of intent with three airports—Boston Logan, Dallas-Fort Worth, and Seattle-Tacoma International Airports. Under the agreements, TSA will pay 75 percent of the cost of integrating the explosives detection equipment into the baggage-handling systems. The payments will stretch out over 3 to 4 years. Airport representatives said that about 30 more airports have

[17]TSA suspended the security fees from June 1 to September 30, 2003, as mandated by the Emergency Wartime Supplemental Appropriations Act of 2003.

[18]With FAA's approval, commercial airports may charge boarding passengers a fee of up to $4.50 per trip segment to raise funds for airport capital development.

[19]A letter of intent represents a nonbinding commitment from an agency to provide multiyear funding to an entity beyond the current authorization period. Thus, that letter allows an airport to proceed with a project without waiting for future federal funds because the airport and investors know that allowable costs are likely to be reimbursed.

[20]U.S. General Accounting Office, *Airport Finance: Past Funding Levels May Not Be Sufficient to Cover Airports' Planned Capital Development*, GAO-03-497T (Washington, D.C.: Feb. 25, 2003).

requested similar agreements. The slow pace of TSA's approval process has raised concerns about delays in reinstalling and integrating explosives detection equipment with baggage-handling systems—delays that will require more labor-intensive and less efficient baggage screening by other approved means.

To provide financial assistance to airports for security-related capital investments, such as the installation of explosives detection equipment, proposed aviation reauthorization legislation[21] would establish an aviation security capital fund that would authorize $2 billion over the next 4 years. The funding would be made available to airports in letters of intent, and large- and medium-hub airports would be expected to provide a match of 10 percent of a project's costs. A 5 percent match would be required for all other airports. This legislation would provide a dedicated source of funding for security-related capital investments and could minimize the need to use AIP funds for security.

An additional funding issue is how to ensure continued investment in transportation research and development. For fiscal year 2003, TSA was appropriated about $110 million for research and development, of which $75 million was designated for the next-generation explosives detection systems. However, TSA has proposed to reprogram $61.2 million of these funds to be used for other purposes, leaving about $12.7 million to be spent on research and development this year. This proposed reprogramming could limit TSA's ability to sustain and strengthen aviation security by continuing to invest in research and development for more effective equipment to screen passengers, their carry-on and checked baggage, and cargo. In ongoing work, we are examining the nature and scope of research and development work by TSA and the Department of Homeland Security, including their strategy for accelerating the development of transportation security technologies.

By reprogramming funds and making acknowledged use of certain funds for purposes other than those intended, TSA has raised congressional concerns about accountability. According to TSA, it has proposed to reprogram a total of $849.3 million during fiscal year 2003, including the $61.2 million that would be cut from research and development and $104 million that would be taken from the federal air marshal program and used for unintended purposes. Because of these congressional concerns, we

[21]The proposed Vision 100—Century of Aviation Reauthorization—Act, H.R. 2115.

were asked to investigate TSA's process for reprogramming funds for the air marshal program and to assess the implications of the proposed funding reductions in areas such as the numbers of hours flown and flights taken. We have ongoing work to address these issues. To ensure appropriate oversight and accountability, it is important that TSA maintain clear and transparent communication with the Congress and industry stakeholders about the use of its funds.

In July 2002, we reported that long-term attention to cost and accountability controls for acquisition and related business processes will be critical for TSA, both to ensure its success and to maintain its integrity and accountability.[22] According to DOT's Inspector General, although TSA has made progress in addressing certain cost-related issues, it has not established an infrastructure that provides effective controls to monitor contractors' costs and performance.[23] For example, in February 2003, the Inspector General reported that TSA's $1 billion hiring effort cost more than most people expected and that TSA's contract with NCS Pearson to recruit, assess, and hire the screener workforce contained no safeguards to prevent cost increases. The Inspector General found that TSA provided limited oversight for the management of the contract expenses and, in one case, between $6 million and $9 million of the $18 million paid to a subcontractor appeared to be a result of wasteful and abusive spending practices.[24] As the Inspector General recommended, TSA has since hired the Defense Contract Audit Agency to audit its major contracts. To ensure control over TSA contracts, the Inspector General has further recommended that the Congress set aside a specific amount of TSA's contracting budget for overseeing contractors' performance with respect to cost, schedule, and quality.[25]

[22]U.S. General Accounting Office, *Aviation Security: Transportation Security Administration Faces Immediate and Long-Term Challenges*, GAO-02-971T (Washington, D.C.: July 25, 2002).

[23]*Aviation Security Costs*, *Transportation Security Administration*, statement of the Honorable Kenneth M. Mead, Inspector General, U.S. Department of Transportation, before the Committee on Commerce, Science and Transportation, Subcommittee on Aviation, U.S. Senate, Feb. 5, 2003 (CC-2003-066).

[24]DOT Inspector General, CC-2003-066.

[25]Office of Inspector General, DOT, *Report on Oversight of Security Screener Contracts*, *TSA*, FI-2003-025 (Washington, D.C.: Feb. 28, 2003).

Coordination

Sustaining the aviation security advancements of the past 2 years also depends on TSA's ability to form effective partnerships with federal, state, and local agencies and with the aviation community. Effective, well-coordinated partnerships at the local level require identifying roles and responsibilities; developing effective, collaborative relationships with local and regional airports and emergency management and law enforcement agencies; agreeing on performance-based standards that describe desired outcomes; and sharing intelligence information. The lynchpin in TSA's efforts to coordinate with airports and local law enforcement and emergency response agencies is, according to the agency, the 158 federal security directors and staff that TSA has deployed nationwide. The security directors' responsibilities include ensuring that standardized security procedures are implemented at the nation's airports; working with state and local law enforcement personnel, when appropriate, to ensure airport and passenger security; and communicating threat information to airport operators and others. Airport representatives, however, have indicated that the relationships between federal security directors and airport operators are still evolving and that better communication is needed at some airports.

Key to improving the coordination between TSA and local partners is establishing clearly defined roles. In some cases, concerns have arisen about conflicts between the roles of TSA, as the manager of security functions at airports, and of airport officials, as the managers of other airport operations. Industry representatives viewed such conflicts as leading to confusion in areas such as communicating with local entities. According to airport representatives, for example, TSA has developed guidance or rules for airports without involving them, and time-consuming changes have then had to be made to accommodate operational factors. The representatives maintain that it would be more efficient and effective to consider such operational factors earlier in the process. Ultimately, inadequate coordination and unclear roles result in inefficient uses of limited resources.

TSA also has to ensure that the terrorist and threat information gathered and maintained by law enforcement and other agencies—including the Federal Bureau of Investigation, the Immigration and Naturalization Service, the Central Intelligence Agency, and the Department of State—is quickly and efficiently communicated among federal agencies and to state and local authorities, as needed. Disseminating such information is important to allow those who are involved in protecting the nation's aviation system to address potential threats rather than simply react to known threats.

In aviation security, timely information sharing among agencies has been hampered by the agencies' reluctance to share sensitive information and by outdated, incompatible computer systems. As we found in reviewing 12 watch lists maintained by nine federal agencies, information was being shared among some of them but not among others. Moreover, even when sharing was occurring, costly and overly complex measures had to be taken to facilitate it.[26] To promote better integration and sharing of terrorist and criminal watch lists, we have recommended that the Department of Homeland Security, in collaboration with the other departments and agencies that have and use watch lists, lead an effort to consolidate and standardize the federal government's watch list structures and policies.[27]

In addition, as we found earlier this year, representatives of numerous state and local governments and transportation industry associations indicated that the general threat warnings received by government agencies are not helpful. Rather, they said, transportation operators, including airport operators, want more specific intelligence information so that they can understand the true nature of a potential threat and implement appropriate security measures.[28]

Strategic Human Capital Management

As it organizes itself to protect the nation's transportation system, TSA faces the challenge of strategically managing its workforce of more than 60,000 people, most of whom are deployed at airports or on aircraft to detect weapons and explosives and to prevent them from being taken aboard and used on aircraft. Additionally, over the next several years, TSA faces the challenge of "right-sizing" this workforce as efficiency is improved with new security-enhancing technologies, processes, and procedures. For example, as explosives detection systems are integrated with baggage-handling systems, the use of more labor-intensive screening methods, such as trace detection techniques and manual searches of baggage, can be reduced. Other planned security enhancements, such as CAPPS II and the registered traveler program, also have the potential to make screening more efficient.

[26]GAO-03-322.

[27]U.S. General Accounting Office, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, GAO-03-322 (Washington, D.C.: Apr. 15, 2003).

[28]GAO-03-843.

To assist agencies in managing their human capital more strategically, we have developed a model that identifies cornerstones and related critical success factors that agencies should apply and steps they can take.[29] Our model is designed to help agency leaders effectively lead and manage their people and integrate human capital considerations into daily decision-making and the program results they seek to achieve.

In January 2003, we reported that TSA was addressing some critical human capital success factors by hiring personnel, using a wide range of tools available for hiring, and beginning to link individual performance to organizational goals.[30] However, concerns remain about the size and training of that workforce, the adequacy of the initial background checks for screeners, and TSA's progress in setting up a performance management system. As noted earlier in this testimony, TSA now plans to reduce its screener workforce by 6,000 by September 30, 2003, and it has proposed cutting the workforce by an additional 3,000 in fiscal year 2004. This planned reduction has raised concerns about passenger delays at airports and has led TSA to begin hiring part-time screeners to make more flexible and efficient use of its workforce. In addition, TSA used an abbreviated background check process to hire and deploy enough screeners to meet ATSA's screening deadlines in 2002. After obtaining additional background information, TSA terminated the employment of some of these screeners. TSA reported 1,208 terminations as of May 31, 2003, that it ascribed to a variety of reasons, including criminal offenses and failures to pass alcohol and drug tests. Furthermore, the national media have reported allegations of operational and management control problems that emerged with the expansion of the Federal Air Marshal Service, including inadequate background checks and training, uneven scheduling, and inadequate policies and procedures. In ongoing work, we are examining the effectiveness of TSA's efforts to train, equip, and supervise passenger screeners, and we are assessing the effects of expansion on the Federal Air Marshal Service. In addition, we reported in January 2003 that TSA had taken the initial steps in establishing a performance management system linked to organizational goals. Such a system will be critical for TSA to motivate and manage staff, ensure the

[29]U.S. General Accounting Office, *A Model of Strategic Human Capital Management*, GAO-02-373SP (Washington, D.C.: March 2002).

[30]U.S. General Accounting Office, *Transportation Security Administration: Actions and Plans to Build a Results-Oriented Culture*, GAO-03-190 (Washington, D.C.: Jan. 13, 2003).

quality of screeners' performance, and, ultimately, restore public confidence in air travel.

Building a Results-Oriented Organization

For TSA to sustain enhanced aviation security over the long term, it will be important for the agency to continue to build a results-oriented culture within the new Department of Homeland Security. To help federal agencies successfully transform their cultures, as well as the new Department of Homeland Security merge its various components into a unified department, we identified key practices that have consistently been found at the center of successful mergers, acquisitions, and transformations.[31] These key practices, together with implementation strategies such as establishing a coherent mission and integrated strategic goals to guide the transformation, can help agencies become more results oriented, customer focused, and collaborative. (See app. III.) These practices are particularly important for the Department of Homeland Security, whose implementation and transformation we have designated as high risk.[32]

The Congress required TSA to adopt a results-oriented strategic planning and reporting framework and, specifically, to provide an action plan with goals and milestones to outline how acceptable levels of performance for aviation security would be achieved. In prior work, we reported that TSA has taken the first steps in performance planning and reporting by defining its mission, vision, and values and that this practice would continue to be important when TSA moved into the Department of Homeland Security.[33] Therefore, we recommended that TSA take the next steps to implement results-oriented practices. These steps included establishing performance goals and measures for all modes of transportation as part of a strategic planning process that involves stakeholders, defining more clearly the roles and responsibilities of its various offices in collaborating and communicating with stakeholders; and formalizing the roles and responsibilities of governmental entities for transportation security. Table

[31]U.S. General Accounting Office, *Results-Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformations*, GAO-03-669 (Washington, D.C.: July 2, 2003).

[32]U.S. General Accounting Office, *Major Management Challenges and Program Risks: Department of Homeland Security*, GAO-03-102 (Washington, D.C.: Jan. 1, 2003).

[33]GAO-03-190.

1 shows selected ATSA requirements, TSA's actions and plans, and the next steps we recommended. TSA agreed with our recommendations.

Table 1: Requirements, Actions and Plans, and Recommended Next Steps for Results-Oriented Practices

ATSA requirements	TSA actions and plans	Next steps
Leadership commitment to creating a high-performing organization		
• Requires performance agreement between the Secretary of DOT and the Under Secretary of Transportation for Security and between the Under Secretary and TSA executives.	• Stated leadership commitment to creating a results-oriented culture in its 180-day action plan. • Expressed plans to use the Baldrige performance excellence criteria as a management tool to promote quality and performance. • Established standardized performance agreements for TSA executives.	• Establish a performance agreement for the Under Secretary of Transportation for Security that articulates how bonuses will be tied to performance. • Add expectations in performance agreements for top leadership to foster the culture of a high-performing organization.
Strategic planning to establish results-oriented goals and measures		
• Requires a 5-year performance plan and annual performance report consistent with the principles of the Government Performance and Results Act.	• Articulated vision, mission, values, strategic goal, and performance goals and measures. • Developed automated system to collect performance data to demonstrate progress in meeting goals. • Aligned aviation security performance goals and measures with DOT goals. • Reported it submitted first annual performance report.	• Establish security performance goals and measures for all modes of transportation as part of a strategic planning process that involves stakeholders. • Apply practices that have been shown to provide useful information in agency performance plans.
Performance management to promote accountability for results		
• Requires a performance management system. • Requires performance agreements for all employees that include organizational and individual goals.	• Established an interim performance management system. • Created standardized performance agreements for groups of employees that include organizational and individual goals and standards of performance.	• Build on the current performance agreements to achieve additional benefits. • Ensure the permanent performance management system makes meaningful distinctions in performance. • Involve employees in developing its permanent performance management system.

ATSA requirements	TSA actions and plans	Next steps
Collaboration and communication to achieve national outcomes		
• Requires TSA to work within and outside the government to accomplish its mission. • Establishes a Transportation Security Oversight Board to facilitate collaboration and communication.	• Established Offices of Security Regulation and Policy, Communications and Public Information, Law Enforcement and Security Liaison, and Legislative Affairs to collaborate and communicate with stakeholders. • Convened the Oversight Board, which has met twice. • Stated plans to use memorandums of understanding and memorandums of agreement to formalize roles and responsibilities of TSA and other agencies in transportation security.	• Define more clearly the collaboration and communication roles and responsibilities of TSA's various offices. • Formalize roles and responsibilities among governmental entities for transportation security.
Public reporting and customer service to build citizen confidence		
• Requires a 180-day action plan and two progress reports within 6 months of enactment.	• Submitted 180-day action plan and both progress reports within established time frames. • Maintains a Web site to provide information to the public. • Created ombudsman position to serve customers. • Developed measures to track customer satisfaction. • Reviewed and eliminated security procedures that do not enhance security or customer service. • Stated plans to develop a customer satisfaction index to analyze customer opinions to improve performance.	• Fill the ombudsman position to facilitate responsiveness of TSA to the public. • Continue to develop and implement mechanisms, such as the CSI, to gauge customer satisfaction and improve customer service.

Source: GAO.

Concluding Observations

After spending billions of dollars over the past 2 years on people, policies, and procedures to improve aviation security, we have much more security now than we had before September 2001, but it has not been determined how much more secure we are. The vast number of guns, knives, and other potential threat items that screeners have confiscated suggests that security is working, but it also suggests that improved public awareness of prohibited items could help focus resources where they are most needed and reduce delays and inconvenience to the public. Faced with vast and competing demands for security resources, TSA should continue its efforts to identify technologies, such as CAPPS II, that will leverage its resources and potentially improve its capabilities. Improving the efficiency and effectiveness of aviation security will also require risk assessments and plans that help maintain a balance between security and customer service.

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

Contact Information

For further information on this testimony, please contact Gerald L. Dillingham at (202) 512-2834. Individuals making key contributions to this testimony include Elizabeth Eisenstadt, David Hooper, Jennifer Kim, Heather Krause, Maren McAvoy, John W. Shumann, and Teresa Spisak.

Appendix I: Selected Deadlines in the Aviation and Transportation Security Act and Their Status

Deadline	Provisions[a]	Status
Nov. 19, 2001	Require new background checks for those who have access to secure areas of the airport.	Completed
	Institute a 45-day waiting period for aliens seeking flight training for planes of 12,500 pounds or more.	Completed
Dec. 19, 2001	Establish qualifications for federal screeners.	Completed
	Report to the Congress on improving general aviation security.	Completed
Jan. 18, 2002	Screen all checked baggage in U.S. airports using explosives detection systems, passenger-bag matching, manual searches, canine units, or other approved means.	Completed
	The Federal Aviation Administration (FAA) is to develop guidance for air carriers to use in developing programs to train flight and cabin crews to resist threats (within 60 days after FAA issues the guidance, each airline is to develop a training program and submit it to FAA; within 30 days of receiving a program, FAA is to approve it or require revisions; within 180 days of receiving FAA's approval, the airline is to complete the training of all flight and cabin crews).	Guidance issued
	Develop a plan to train federal screeners.	Completed
	Foreign and domestic carriers are to provide electronic passenger and crew manifests to Customs for flights from foreign countries to the United States.	Completed
	Begin collecting the passenger security fee.	Completed
Feb. 17, 2002	The Under Secretary is to assume civil aviation security functions from FAA.	Completed
	Implement an aviation security program for charter carriers.	Completed
	Begin awarding grants for security-related research and development.	Completed
	The National Institute of Justice is to report to the Secretary on less-than-lethal weapons for flight crew members.	Completed
May 18, 2002	Report to the Congress on the deployment of baggage screening equipment.	Report submitted
	• Report to the Congress on progress in evaluating and taking the following optional actions:	Report submitted
	• Require 911 capability for onboard passenger telephones.	• Completed
	• Establish uniform IDs for law enforcement personnel carrying weapons on planes or in secure areas.	• Ongoing
	• Establish requirements for trusted traveler programs.	• Ongoing
	• Develop alternative security procedures to avoid damage to medical products.	• Completed
	• Provide for the use of secure communications technologies to inform airport security forces about passengers who are identified on security databases.	• Ongoing
	• Require pilot licenses to include a photograph and biometric identifiers.	• Ongoing
	• Use voice stress analysis, biometric, or other technologies to prevent high-risk passengers from boarding.	• Ongoing
	• Provide for the use of instant communications technology between planes and ground.	• Ongoing

Deadline	Provisions[a]	Status
Nov. 19, 2002	Deploy federal screeners, security managers, and law enforcement officers to screen passengers and property.	Completed
	Report to the Congress on screening for small aircraft with 60 or fewer seats.	Report submitted
	Establish pilot program to contract with private screening companies (program to last until Nov. 19, 2004).	Completed
Dec. 31, 2002	Screen all checked baggage by explosives detection systems.	Ongoing
No deadline	Carriers are to transfer screening property to TSA.	Completed
	FAA is to issue an order prohibiting access to the flight deck, requiring strengthened cabin doors, requiring that cabin doors remain locked, and prohibiting possession of a key for all but the flight deck crew.	Completed
	Improve perimeter screening of all individuals, goods, property, and vehicles.	Ongoing
	Screen all cargo on passenger flights and cargo-only flights.	Ongoing
	Establish procedures for notifying FAA, state and local law enforcement officers, and airport security of known threats.	Completed
	Establish procedures for airlines to identify passengers who pose a potential security threat.	Ongoing
	FAA is to develop and implement methods for using cabin video monitors, continuously operating transponders, and notifying flight deck crew of a hijacking.	Ongoing
	Require flight training schools to conduct security awareness programs for employees.	Completed
	Work with airport operators to strengthen access control points and consider deploying technology to improve security access.	Ongoing
	Provide operational testing for screeners.	Ongoing
	Assess dual-use items that seem harmless but could be dangerous and inform screening personnel.	Ongoing
	Establish a system for measuring staff performance.	Ongoing
	Establish management accountability for meeting performance goals.	Ongoing
	Periodically review threats to civil aviation, including chemical and biological weapons.	Ongoing

Source: TSA.

[a]Except where otherwise indicated, the Transportation Security Administration (TSA) is responsible for implementing the provisions.

Appendix II: Bills Related to Aviation Security

H.R. 2144 - Aviation Security Technical Corrections and Improvements Act - Many of the important provisions of this bill have been incorporated into the Conference Report version of the FAA Reauthorization Act, H.R. 2115.

S. 1409 - Rebuild America Act of 2003 - Establishes a new grant program in the Department of Homeland Security (DHS) for airport security improvements, including projects to replace baggage conveyer systems and projects to reconfigure terminal baggage areas as needed to install explosives detection systems. The Under Secretary for Border and Transportation Security is authorized to issue letters of intent to airports for these types of projects. One billion dollars is authorized for this program.

H.R. 2555 - House and Senate versions of the Department of Homeland Security Appropriations Act for 2004

House version - Makes fiscal year 2004 appropriations of $3.679 billion for the Transportation Security Administration (TSA) to provide civil aviation security services (aviation security, federal air marshals, maritime and land security, intelligence, research and development, and administration):

- $1.673 billion for passenger screening activities,
- $1.285 billion for baggage screening activities,
- $721 million for airport support and enforcement presence,
- $235 million for physical modifications of airports to provide for the installation of checked baggage explosives detection systems, and
- $100 million for the procurement of the explosives detection systems.

Continues to cap the number of screeners at 45,000 full-time equivalent positions.

Prohibits the use of funds authorized in this act to pursue or adopt regulations requiring airport sponsors to provide, without cost to TSA, building construction, maintenance, utilities and expenses, or space for services relating to aviation security (excluding space for necessary checkpoints).

Senate Version of H.R. 2555 - Makes fiscal year 2004 appropriations of $4.524 billion for TSA to provide civil aviation security services:

- $3.185 billion for screening activities,

- $1.339 billion for airport support and enforcement presence,
- $309 million for physical modifications of airports to provide for the installation of checked baggage explosives detection systems, and
- $151 million for the procurement of the explosives detection systems.

Prohibits the use of funds authorized in this act to pursue or adopt regulations requiring airport sponsors to provide, without cost to TSA, building construction, maintenance, utilities and expenses, or space for services relating to aviation security (excluding space for necessary checkpoints).

Prohibits the use of funds authorized in this act for the Computer Assisted Passenger Prescreening System (CAPPS II) until GAO has reported to the Committees on Appropriations that certain requirements have been met, including (1) the existence of a system of due process by which passengers considered to pose a threat may appeal their delay or prohibition from boarding a flight; (2) that the underlying error rate of databases will not produce a large number of false positives that will result in a significant number of passengers being treated mistakenly or security resources being diverted; (3) that TSA has stressed-tested and demonstrated the efficacy and predictive accuracy of all search tools in CAPPS II; and (4) that the Secretary has established an internal oversight board to monitor the manner in which CAPPS II is being developed and prepared.

Requires a report from the Secretary of Homeland Security on actions taken to develop countermeasures for commercial aircraft against shoulder-fired missile systems and vulnerability assessments of this threat for larger airports.

H.R. 2115 - Flight 100 - Century of Aviation Reauthorization Act - Conference Report version - Gives FAA the authority to take a certificate action if it is notified by DHS that the holder of the certificate presents a security threat.

Gives the Secretary of Transportation the authority to make grants to general aviation entities (including airports, operators, and manufacturers) to reimburse them for security costs incurred and revenues lost because of restrictions imposed by the federal government in response to the events of September 11. The bill authorizes $100 million for these grants.

Authorizes DHS to reimburse air carriers and airports for all security screening activities they are still performing, such as for providing catering

services and checking documents at security checkpoints and for providing the space and facilities used to perform screening functions to the extent funds are available.

Requires air carriers to carry out a training program for flight and cabin crews to prepare for possible threat conditions. TSA is required to establish minimum standards for this training within 1 year of the act's passage.

Requires DHS to report in 6 months on the effectiveness of aviation security, specifically including the air marshal program; hardening of cockpit doors; and security screening of passengers, checked baggage, and cargo.

Establishes within DHS a grant program to airport sponsors for (1) projects to replace baggage conveyer systems related to aviation security; (2) projects to reconfigure terminal baggage areas as needed to install explosives detection systems; and (3) projects to enable the Under Secretary for Border and Transportation Security to deploy explosives detection systems behind the ticket counter, in the baggage sorting area, or in line with the baggage handling system. Requires $250 million annually from the existing aviation security fee that is paid by airline passengers to be deposited in an Aviation Security Capital Fund and made available to finance this grant program.

Requires TSA to certify that civil liberty and privacy issues have been addressed before implementing CAPPS II and requires GAO to assess TSA's compliance 3 months after TSA makes the required certification.

Allows cargo pilots to carry guns under the same program for pilots of passenger airlines. Permits an off-duty pilot to transport the gun in a lockbox in the passenger cabin rather than in the baggage hold. Also provides that both passenger and cargo pilots should be treated equitably in their access to training.

Requires security audits of all foreign repair stations within 18 months after TSA issues rules governing the audits. The rules must be issued within 240 days of enactment.

Requires background checks on aliens seeking flight training in aircraft regardless of the size of the aircraft. For all training on small aircraft, includes a notification requirement but no waiting period. For training on larger aircraft, adopts an expedited procedure if the applicant already has

training, a license, or a background check, and adopts a 30-day waiting period for first-time training on large aircraft. Makes TSA responsible for the background check. Requires TSA to issue an interim final rule in 60 days to implement this section. This section takes effect when that rule becomes effective.

S.236 - Background Checks for Foreign Flight School Applicants - Amends federal aviation law to require a background check of alien flight school applicants without regard to the maximum certificated weight of the aircraft for which they seek training. (Currently, a background check is required for flight crews operating aircraft with a maximum certificated takeoff weight of 12,500 pounds or more.)

S. 165 - Air Cargo Security Act - House companion bill (H.R. 1103) - Amends federal aviation law to require the screening of cargo that is to be transported in passenger aircraft operated by domestic and foreign air carriers in interstate air transportation. Directs TSA to develop a strategic plan to carry out such screening. Requires the establishment of systems that (1) provide for the regular inspection of shipping facilities for cargo shipments; (2) provide an industrywide pilot program database of known shippers of cargo; (3) train persons that handle air cargo to ensure that such cargo is properly handled and safeguarded from security breaches; and (4) require air carriers operating all-cargo aircraft to have an approved plan for the security of their air operations area, the cargo placed aboard the aircraft, and persons having access to their aircraft on the ground or in flight.

H.R. 1366 - Aviation Industry Stabilization Act - Requires the Under Secretary for Border and Transportation Security, after all cockpit doors are strengthened, to consider and report to the Congress on whether it is necessary to require federal air marshals to be seated in the first class cabin of an aircraft with strengthened cockpit doors.

Requires the Under Secretary to (1) undertake action necessary to improve the screening of mail so that it can be carried on passenger flights and (2) reimburse air carriers for certain screening and related activities, as well as the cost of fortifying cockpit doors, and for any financial losses attributed to the loss of air traffic resulting from the use of force against Iraq in calendar year 2003.

Establishes an air cargo security working group composed of various groups to develop recommendations on the enhancement of the current known shipper program.

H. R. 115 - Aviation Biometric Badge Act - Amends federal aviation law to direct TSA to require by regulation that each security screener (or employee who has unescorted access, or may permit other individuals to have unescorted access, to an aircraft or a secured area of the airport) be issued a biometric security badge that identifies a person by fingerprint or retinal recognition.

H. R. 1049 - Arming Cargo Pilots Against Terrorism Act - Senate companion bill (S. 516) - Expresses the sense of Congress that a flight deck crew member of a cargo aircraft should be armed with a firearm to defend such aircraft against attacks by terrorists that could use the aircraft as a weapon of mass destruction or for other terrorist purposes. Amends federal transportation law to authorize the training and arming of flight deck crew members (pilots) of all-cargo air transportation flights to prevent acts of criminal violence or air piracy.

H.R. 765 - (No title) - Legislation to arm cargo pilots - Amends federal aviation law to allow cargo pilots (not just air passenger pilots) to participate in the federal flight deck officer program.

H.R. 580 - Commercial Airline Missile Defense Act - Senate companion bill - S. 311 - Directs the Secretary of Transportation to issue regulations that require all turbojet aircraft of air carriers to be equipped with a missile defense system. Requires the Secretary to purchase such defense systems and make them available to all air carriers. Sets forth certain interim security measures to be taken before the deployment of such defense systems.

Appendix III: Key Practices and Implementation Steps for Mergers and Organizational Transformations

Practice	Implementation step
Ensure top leadership drives the transformation.	• Define and articulate a succinct and compelling reason for change. • Balance continued delivery of services with merger and transformation activities.
Establish a coherent mission and integrated strategic goals to guide the transformation.	• Adopt leading practices for results-oriented strategic planning and reporting.
Focus on a key set of principles and priorities at the outset of the transformation.	• Embed core values in every aspect of the organization to reinforce the new culture.
Set implementation goals and a time line to build momentum and show progress from day one.	• Make public implementation goals and a time line. • Seek and monitor employee attitudes and take appropriate follow-up actions. • dentify cultural features of merging organizations to increase understanding of former work environments. • Attract and retain key talent. • Establish an organizationwide knowledge and skills inventory to exchange knowledge among merging organizations.
Dedicate an implementation team to manage the transformation process.	• Establish networks to support the implementation team. • Select high-performing team members.
Use the performance management system to define responsibility and ensure accountability for change.	• Adopt leading practices to implement effective performance management systems with adequate safeguards.
Establish a communication strategy to create shared expectations and report related progress.	• Communicate early and often to build trust. • Ensure consistency of message. • Encourage two-way communication. • Provide information to meet specific needs of employees.
Involve employees to obtain their ideas and gain their ownership for the transformation.	• Use employee teams. • Involve employees in planning and sharing performance information. • Incorporate employee feedback into new policies and procedures. • Delegate authority to appropriate organizational levels.
Build a world-class organization.	• Adopt leading practices to build a world-class organization.

Source: GAO.

Appendix IV: GAO Active Engagements Related to Aviation Security

Transportation Security Research and Development Programs at DHS and TSA

Key Questions: (1) What were the strategy and organizational structure for transportation security research and development (R&D) prior to 9/11 and what is the current strategy and structure? (2) How do DHS and TSA select their transportation security R&D projects and what projects are in their portfolios? (3) What are DHS's and TSA's goals and strategies for accelerating the development of transportation security technologies? (4) What are the nature and scope of coordination of R&D efforts between DHS and TSA, as well as with other public and private sector research organizations?

Federal Air Marshal Service

Key Questions: (1) How has the federal air marshal program evolved, in terms of recruiting, training, retention, and operations since its management was transferred to TSA? (2) To what extent has TSA implemented the internal controls needed to meet the program's operational and management control challenges? (3) To what extent has TSA developed plans and initiatives to sustain the program and accommodate its future growth and maturation?

TSA Baggage Screening

Key Questions: (1) What are the status and associated costs of TSA's efforts to acquire, install, and operate explosives detection equipment (electronic trace detection technology and explosives detection systems) to screen all checked baggage by December 31, 2003? (2) What are the benefits and trade-offs—to include costs, operations, and performance—of using alternative explosives detection technologies currently available for baggage screening?

Reprogramming of Air Marshal Program Funds

Key Questions: (1) Describe the internal preparation, review, and approval process for DHS's reprogrammings and, specifically, the process for the May 15 and July 25 reprogramming requests for the air marshal program. (2) Determine whether an impoundment or deferral notice should have been sent to the Congress and any other associated legal issues. (3) Identify the implications, for both the air marshal program and other programs, of the pending reprogramming request.

General Aviation Security

Key Questions: (1) How have security concerns and measures changed at general aviation airports since September 11, 2001? (2) What steps has TSA taken to improve general aviation security?

Background Checks for Banner-Towing Aircraft

Key Questions: (1) What are the procedures for conducting background and security checks for pilots of small banner-towing aircraft requesting waivers to perform stadium overflights? (2) To what extent have these procedures been followed in conducting required background and security checks since September 11, 2001? (3) How effective have these procedures been in reducing risks to public safety?

TSA's Computer Assisted Passenger Prescreening System II (CAPPS II)

Key Questions: (1) How will the CAPPS II system function and what data will be needed to make the system operationally effective? (2) What safeguards will be put in place to protect the traveling public's privacy? (3) What systems and measures are in place to determine whether CAPPS II will result in improved national security? (4) What impact will CAPPS II have on the traveling public and on the airline industry in terms of costs, delays, risks, inconvenience, and other factors?

TSA Passengers Screening Program

*Key Questions: (*1) What efforts have been taken or planned to ensure that passenger screeners comply with federal standards and other criteria, including efforts to train, equip, and supervise passenger screeners? (2) What methods does TSA use to test screeners' performance, and what have been the results of these tests? (3) How have the results of tests of TSA passenger screeners compared with the results achieved by screeners before September 11, 2001, and at five pilot program airports? (4) What actions is TSA taking to remedy performance concerns?

TSA's Efforts to Implement Sections 106, 136, and 138 of the Aviation and Transportation Security Act

Key Questions: What is the status of TSA's efforts to implement (1) section 106 of the act requiring improved airport perimeter access security, (2) section 136 requiring the assessment and deployment of

commercially available security practices and technologies, and (3) section 138 requiring background investigations for TSA and other airport employees?

Assessment of the Portable Air Defense Missile Threat

Key Questions: (1) What are the nature and extent of the threat from man-portable air defense systems (MANPAD)? (2) How effective are U.S. controls on the use of exported MANPADs? (3) How do multilateral efforts attempt to stem MANPAD proliferation? (4) What types of countermeasures are available to minimize this threat and at what cost?

Airline Assistance Determination of Whether the $5 Billion Provided by P.L. 107-42 Was Used to Compensate the Nation's Major Air Carriers for Their Losses Stemming from the Events of Sept. 11, 2001

Key Questions: (1) Was the $5 billion used only to compensate major air carriers for their uninsured losses incurred as a result of the terrorist attacks? (2) Were carriers reimbursed, per the act, only for increases in insurance premiums resulting from the attacks?

TSA's Use of Sole-Source Contracts

Key Questions: (1) To what extent does TSA follow applicable acquisition laws and policies, including those for ensuring adequate competition? (2) How well does TSA's organizational structure facilitate effective, efficient procurement? (3) How does TSA ensure that its acquisition workforce is equipped to award and oversee contracts? (4) How well do TSA's policies and processes ensure that TSA receives the supplies and services it needs on time and at reasonable cost?

Related GAO Products

Aviation Security

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. GA0-02-822R. 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)

Computer Security: FAA Is Addressing Personnel Weaknesses, but Further Action Is Required. GAO/AIMD-00-169. Washington, D.C.: May 31, 2000.

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

Aviation Security: Screener Performance in Detecting Dangerous Objects during FAA Testing Is Not Adequate. GAO/T-RCED-00-143. Washington, D.C.: April 6, 2000. (NOT FOR PUBLIC DISSEMINATION)

Combating Terrorism: How Five Foreign Countries Are Organized to Combat Terrorism. GAO/NSIAD-00-85. Washington, D.C.: April 7, 2000.

Aviation Security: Vulnerabilities Still Exist in the Aviation Security System. GAO/T-RCED/AIMD-00-142. Washington, D.C.: April 6, 2000.

U.S. Customs Service: Better Targeting of Airline Passengers for Personal Searches Could Produce Better Results. GAO/GGD-00-38. Washington, D.C.: March 17, 2000.

Aviation Security: Screeners Not Adequately Detecting Threat Objects during FAA Testing. GAO/T-RCED-00-124. Washington, D.C.: March 16, 2000. (NOT FOR PUBLIC DISSEMINATION)

Aviation Security: Slow Progress in Addressing Long-Standing Screener Performance Problems. GAO/T-RCED-00-125. Washington, D.C.: March 16, 2000.

Computer Security: FAA Needs to Improve Controls Over Use of Foreign Nationals to Remediate and Review Software. GAO/AIMD-00-55. Washington, D.C.: December 23, 1999.

Aviation Security: FAA's Actions to Study Responsibilities and Funding for Airport Security and to Certify Screening Companies. GAO/RCED-99-53. Washington, D.C.: February 24, 1999.

Aviation Security: FAA's Deployments of Equipment to Detect Traces of Explosives. GAO/RCED-99-32R. Washington, D.C.: November 13, 1998.

Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety. GAO/AIMD-98-155. Washington, D.C.: May 18, 1998.

Aviation Security: Progress Being Made, but Long-Term Attention Is Needed. GAO/T-RCED-98-190. Washington, D.C.: May 14, 1998.

Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety. GAO/AIMD-98-60. Washington, D.C.: April 29, 1998. (LIMITED OFFICIAL USE –DO NOT DISSEMINATE)

Aviation Security: Implementation of Recommendations Is Under Way, but Completion Will Take Several Years. GAO/RCED-98-102. Washington, D.C.: April 24, 1998.

Combating Terrorism: Observations on Crosscutting Issues. T-NSIAD-98-164. Washington, D.C.: April 23, 1998.

Aviation Safety: Weaknesses in Inspection and Enforcement Limit FAA in Identifying and Responding to Risks. GAO/RCED-98-6. Washington, D.C.: February 27, 1998.

Aviation Security: FAA's Procurement of Explosives Detection Devices. GAO/RCED-97-111R. Washington, D.C.: May 1, 1997.

Aviation Security: Commercially Available Advanced Explosives Detection Devices. GAO/RCED-97-ll9R. Washington, D.C.: April 24, 1997.

Aviation Safety and Security: Challenges to Implementing the Recommendations of the White House Commission on Aviation Safety and Security. GAO/T-RCED-97-90. Washington, D.C.: March 5, 1997.

Aviation Security: Technology's Role in Addressing Vulnerabilities. GAO/T-RCED/NSIAD-96-262. Washington, D.C.: September 19, 1996.

Aviation Security: Oversight of Initiatives Will Be Needed. C-GAO/T-RCED/NSIAD-96-20. Washington, D.C.: September 17, 1996. (CLASSIFIED)

Aviation Security: Urgent Issues Need to Be Addressed. GAO/T-RCED/NSIAD-96-251. Washington, D.C.: September 11, 1996.

Aviation Security: Immediate Action Needed to Improve Security. GAO/T-RCED/NSIAD-96-237. Washington, D.C.: August 1, 1996.

Aviation Security: FAA Can Help Ensure That Airports' Access Control Systems Are Cost Effective. GAO/RCED-95-25. Washington, D.C.: March 1, 1995.

Aviation Security: Development of New Security Technology Has Not Met Expectations. GAO/RCED-94-142. Washington, D.C.: May 19, 1994.

Aviation Security: Additional Actions Needed to Meet Domestic and International Challenges. GAO/RCED-94-38. Washington, D.C.: January 27, 1994.

Other

Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues. GAO-03-715T. Washington, D.C.: May 3, 2003.

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

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

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

Major Management Challenges and Program Risks: Department of Homeland Security. GAO-03-102. Washington, D.C.: January 1, 2003.

Major Management Challenges and Program Risks: Department of Transportation. GAO-03-108. Washington, D.C.: January 2003.

National Preparedness: Integration of Federal, State, Local, and Private Sector Efforts Is Critical to an Effective National Strategy for Homeland Security. GAO-02-621T. Washington, D.C.: April 11, 2002.

Homeland Security: Progress Made, More Direction and Partnership Sought. GAO-02-490T. Washington, D.C.: March 12, 2002.

A Model of Human Capital Management. GAO-02-373SP. Washington, D.C.: March 2002.

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