



## Testimony

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

---

For Release on Delivery  
Expected at  
9:30 a.m. EDT  
Thursday  
July 25, 2002

# AVIATION SECURITY

## Transportation Security Administration Faces Immediate and Long- Term Challenges

Statement of Gerald L. Dillingham,  
Director, Physical Infrastructure Issues



Mr. Chairman and Members of the Committee:

Nearly a year has passed since the terrorist attacks of September 11 turned commercial aircraft into missiles, killing thousands of people, destroying billions of dollars' worth of property, and realigning our national priorities. With these attacks, the safety and security of the nation's civil aviation system assumed greater importance, and efforts to strengthen the system were the subject of much congressional attention. Through dozens of reports and testimonies published since the early 1990s (see app. I), we have contributed to the national discussion on aviation security and to the reforms enacted last November in the Aviation and Transportation Security Act (the act).<sup>1</sup> Among these reforms was the creation of the Transportation Security Administration (TSA), which was assigned responsibility for security in aviation and other modes of transportation. The act also set forth deadlines by which TSA was to implement specific improvements to aviation security.

We are pleased to be here today to discuss TSA's progress in enhancing aviation security and in implementing the act's provisions for addressing security weaknesses in aviation and other modes of transportation. Our testimony, which is based on our prior work as well as our ongoing work for this Committee, includes observations about (1) what TSA has done since September 11 to strengthen aviation security, (2) what immediate challenges TSA faces to strengthen transportation security, and (3) what longer-term challenges TSA can anticipate as it organizes itself to enhance security in all modes of transportation.

In summary:

- Since September 11, TSA has assumed responsibility for aviation security and focused on meeting congressionally mandated deadlines for strengthening aviation security. TSA's accomplishments to date include

---

<sup>1</sup>P.L. 107-71, November 19, 2001.

developing plans and implementing procedures for using federal workers to conduct security screening at 429 commercial airports; hiring and beginning to train almost 4,000 key security personnel; and implementing more rigorous background checks of employees with access to secure areas of airports. TSA faces an extraordinary challenge in hiring and training 33,000 federal workers to conduct passenger security screening by November 19. As of July 13, TSA had hired only 2,475. In addition, deploying explosive detection systems to screen all checked bags by December 31 poses major challenges. Of approximately 1,100 explosive detection systems and 6,000 explosive trace detection machines TSA plans to purchase and deploy at 429 airports, only 200 explosive detection systems and 200 trace detection machines were in use at 56 airports as of June 12, 2002. It is currently uncertain whether, by December 31, TSA can purchase the remaining equipment and hire enough staff to operate and maintain the equipment, whether airports can complete and pay for any modifications required to install the equipment, and whether the equipment will operate as intended.

- TSA faces immediate challenges in assuming responsibility for security in other transportation modes, in improving screeners' performance, and in addressing aviation security issues not covered by the act's current-year deadlines. First, while TSA has begun to coordinate and cooperate with DOT's modal administrations and with other federal agencies, most of the work with these agencies lies ahead. Second, other aviation security challenges facing TSA include improving screeners' ability to detect weapons and explosives and to conduct screening in accordance with federal requirements. Recent TSA tests showed, for example, that screeners at 32 of the nation's largest airports failed to detect fake weapons and explosives in almost a quarter of the tests, and observations by the DOT Inspector General found that contract screeners were not consistently following federal screening requirements. While newly hired

federal screeners are being trained to follow these requirements, contract screeners are still conducting screening at most U.S. airports and have not received upgraded training. Third, other actions are required or have been proposed: for example, the act requires TSA to improve cargo security, and proposed legislation would require TSA to authorize the arming of pilots.

- TSA faces several longer-term challenges as it organizes itself to protect the nation's transportation system. These challenges include strategically managing the workforce, controlling costs, and sharing threat information. TSA is charged with creating a federal screener workforce to replace a private workforce that had been plagued by performance and retention problems. In addition, long-term attention to strong systems and controls for acquisition and related business processes will be critical both to ensuring TSA's success and to maintaining its integrity and accountability. Such attention includes establishing cost control mechanisms and monitoring contractors' performance with respect to cost, schedule, and quality. This is particularly important because of TSA's large acquisition and personnel needs. Finally, the agency depends on access to timely, accurate information about threats, but information sharing among agencies that gather and maintain such information has been hampered by organizational cultures that make agencies reluctant to share sensitive information and by outdated, incompatible computer systems.

## **Background**

The task of securing the nation's aviation system is unquestionably daunting. The enormous size of U.S. airspace defies easy protection. Furthermore, given this country's hundreds of commercial airports, thousands of planes, and tens of thousands of daily flights, as well as the seemingly limitless means terrorists or criminals can devise to attack the system, aviation security must be enforced on

numerous fronts. Safeguarding airplanes and passengers requires, at the least, ensuring that perpetrators are kept from breaching security checkpoints and gaining access to aircraft. The Federal Aviation Administration (FAA), which was responsible for aviation security before TSA was created, developed several mechanisms to prevent criminal attacks on aircraft, such as adopting technology to detect explosives and matching boarding passes to identification cards at the gate to ensure that passengers are positively identified before boarding a flight.

Despite the development of these preventative measures, we and others often demonstrated that significant, long-standing aviation security vulnerabilities existed. These vulnerabilities included inadequate controls for limiting access to secure areas at airports, failure to detect threats when screening passengers and their carry-on bags before they board aircraft, and the absence of any requirement to screen checked baggage on domestic flights. As we reported in May 2000,<sup>2</sup> our special agents used counterfeit law enforcement badges and credentials to gain access to secure areas at two airports, bypassing security checkpoints and walking unescorted to aircraft departure gates. The agents, who had been issued tickets and boarding passes, could have carried weapons, explosives, or other dangerous objects onto aircraft. In addition, FAA's tests of screeners found that their abilities to detect test threat objects located on passengers or contained in their carry-on luggage declined during the 1980s and 1990s, and this problem persists today.

Over the years, plans were developed to address some of these vulnerabilities, but they were not implemented promptly or at all. For example, the Federal Aviation Reauthorization Act of 1996 authorized a certification program that would have established performance, training, and equipment standards for screening companies, but FAA never issued final regulations for the program. In addition, many initiatives were not linked to specific deadlines, making it more difficult to monitor and oversee their implementation.

On November 19, 2001, the Congress passed the Aviation and Transportation Security Act, which created TSA within the Department of Transportation (DOT) and defined its primary responsibility as ensuring security in all modes of transportation. The act also shifted responsibility for the security screening of air passengers and their baggage from the airlines to the federal government, making TSA responsible for overseeing screeners. Finally, the act established a series of requirements for the new agency with mandated deadlines (see app. II), the most important of which are

- to deploy federal screeners at 429 commercial airports across the nation by November 19, 2002, and
- to have explosive detection systems in place at these airports for screening every piece of checked baggage for explosives not later than December 31, 2002.

Recent proposals would move TSA to the proposed Department of Homeland Security.

To help fund its security initiatives, the act authorized air carriers to collect a fee for passengers of \$2.50 per flight segment, not to exceed \$5.00 per one-way trip or \$10.00 per round trip. In addition, the act authorized the Under Secretary of Transportation Security to impose a fee on air carriers if revenues from the new security fee were insufficient to meet the needs mandated by the act. For fiscal year 2002, TSA is seeking a total of \$6.8 billion in appropriated funds--\$2.4 billion of which has already been appropriated and an additional \$4.4 billion in supplemental funding.

---

<sup>2</sup>See U.S. General Accounting Office, GAO-OSI-0010, *Security: Breaches at Federal Agencies and Airports* (Washington, D.C.: May 25, 2002).

## **TSA Has Begun to Address Known Weaknesses in Aviation Security but Is Having Problems Meeting Key Congressional Deadlines**

TSA has begun addressing weaknesses in aviation security but may encounter problems in meeting key congressional deadlines. In the 10 months since September 11, TSA has focused on meeting congressionally mandated deadlines for assuming security responsibilities, upgrading aviation security measures, and reporting to the Congress on its progress. Among other accomplishments, TSA has assumed responsibility for overseeing security screening at 429 commercial airports, established qualifications for federal screeners, developed a plan to hire and train federal screeners, contracted with companies that screen passengers, and overseen the implementation of a variety of federally approved methods to check all bags for explosives. As of July 13, 2002, TSA had also hired about 4,000 staff, including nearly 2,500 passenger screeners, 1,034 former employees of FAA, and 529 other staff. These other staff included federal security directors for airports, attorneys, program analysts, computer information technology specialists, personnel specialists, and administrative staff. In addition, TSA has made significant progress in expanding the federal air marshals service.<sup>3</sup> Finally, TSA has worked with airlines to implement critical interim security measures, such as strengthening cockpit doors.

However, TSA has encountered problems in responding to the congressional mandates that it federalize the screener workforce by November 19, 2002, and provide for screening all checked baggage using explosive detection systems by December 31, 2002.

### **Difficulties in Hiring and Training Passenger Screeners Pose Challenges for TSA**

Initial difficulties in hiring and training the passenger screener workforce will make it challenging for TSA to meet the deadline for federalizing this workforce.

---

<sup>3</sup>Because the number of federal air marshals is classified information, their numbers are not included in the total for employees hired by TSA.

According to TSA's estimates, this effort will involve hiring and training an estimated 33,000 passenger screeners so that 429 commercial airports can be staffed with federal screeners. TSA planned to hire 3,700 passenger screeners and supervisory screeners during May and projected that it would then need to hire and train more than 5,000 passenger screeners a month from June through November. As of July, TSA had hired only 2,475 screeners in total. Because of delays, the DOT Inspector General now estimates that TSA will need to hire 7,600 passenger screeners each month to meet the deadline.

### TSA Faces Difficulties in Meeting Baggage Screening Deadline

TSA faces several challenges in trying to provide for screening 100 percent of checked baggage using explosive detection systems by the end of calendar year 2002. To accomplish this mandate, TSA plans to purchase and deploy an estimated 1,100 bulk explosive detection systems (EDS) and 6,000 explosive trace detection machines (trace devices). The installation of the large EDS equipment may require significant modifications to airports. As of June 12, 2002, 200 EDS and 200 trace devices were being used at 56 airports to screen checked baggage. To expedite installations at other airports, TSA has hired the Boeing Service Company to (1) conduct site assessments at over 400 airports, (2) submit proposals to TSA on what equipment each airport will have and where that equipment will be installed, (3) modify facilities to accommodate this equipment, (4) install and make the equipment operational, (5) maintain the equipment, and (6) train approximately 30,000 screeners to operate the equipment. Given the magnitude of this task, it is unclear whether enough bulk EDS machines can be manufactured, deployed, and operationally tested and whether enough staff can be hired and trained to use the bulk EDS and trace devices by the deadline. Finally, the performance of the existing technologies for detecting explosives has been less than optimal: for example, the machines frequently sound false alarms.

Furthermore, TSA's decision to deploy a combination of bulk EDS and trace devices could have long-term budgetary implications. Although funding is available for airports to purchase the equipment, no specific funding has been provided for airport modifications. These modifications are expected to cost millions of dollars at some major airports. In addition, TSA's plan to install bulk EDS in airport lobbies first and then to move them to the baggage handling areas at certain airports will involve additional costs. It is unclear how much this relocation will cost or who will pay for it. Furthermore, the initial procurement costs may quickly be overshadowed by the costs of the personnel needed to operate the equipment, which might exceed \$1.6 billion each year.

Given the cost of procuring, installing, and operating bulk EDS and trace devices to examine all checked baggage, some security experts and academicians have suggested that an alternative be considered. These individuals advocate adopting a risk-based approach that would match resources to risk levels by establishing a screening process that begins with passengers and concludes with baggage. First, with the use of computer-assisted passenger screening,<sup>4</sup> they believe that passengers could be sorted into different risk groups, such as those who might represent a threat, those about whom little is known, and those about whom enough is known to make them low risk. Second, baggage-screening resources could be targeted according to risk. The passengers who might represent a threat, for instance, could be personally screened, and all available tools (such as explosive detection equipment and manual searches) could be used to ensure that no explosives were present in their checked baggage. The stated advantage of such an approach is that fewer expensive bulk EDS may be needed and the costs may be lower than TSA is projecting. In addition, advocates believe that more cost-effective decisions can be made to replace equipment as newer technologies become available. Conversely, concerns have been raised by TSA and others that the suggested approach increases the risk of not detecting explosives because, for

---

<sup>4</sup>Computer-assisted passenger screening is an automated procedure that reviews data in airline passenger records to identify passengers who might present a risk.

the first level of screening, it uses technology that can screen large numbers of passenger bags quickly but may be less effective in detecting explosives.

### **Many Immediate Challenges Remain to Improve Transportation Security**

Many immediate challenges remain for TSA to improve both the security of other modes of transportation and to strengthen aviation security in areas not covered by specific deadlines. TSA has not yet assumed full responsibility for the security of other modes of transportation, such as highways, railroads, mass transit, ports, and pipelines; however, it has established a number of functions to collaborate and communicate with the DOT agencies responsible for these other modes, as well as with other government agencies. For example, TSA officials told us that the agency has created a broad memorandum of understanding with the U.S. Coast Guard that will serve as a template for such agreements between TSA and other agencies, including the Federal Transit Administration (FTA) and the Federal Bureau of Investigation (FBI). In addition, other DOT modal agencies have various initiatives under way to improve security during this transition period. FTA has, for example, launched a multipart initiative to assess the security of over 30 transit agencies, provide free emergency preparedness and security training for transit agency personnel and first responders, and make grants available for organizing and conducting emergency response drills. Similarly, the U.S. Coast Guard has acted as a focal point for assessing and addressing security concerns for the nation's ports.

Other challenges also confront TSA as it attempts to strengthen aviation security. Passenger screeners still fail to detect weapons and other threat objects (e.g., knives, scissors, and sharp objects) at unacceptable rates, and enhanced screening procedures are unevenly applied among airports. In November 2001, staff from the DOT Inspector General's office observed private contractors carry out screening at 58 security checkpoints and concluded that they were not consistently and uniformly following FAA's screening requirements. For example,

in some cases screeners were not checking passengers' identification against their boarding passes, were not adequately screening carry-on bags for threat objects, and were not performing continuous random secondary screening measures, such as manually searching carry-on items or using wands to screen passengers.

Recent TSA testing found that screeners at 32 of the nation's largest airports failed to detect fake weapons (guns, dynamite, or bombs) in almost a quarter of the undercover tests at screening checkpoints. Since TSA took over aviation security responsibilities on February 17, 2002, discoveries of guns, knives, and other potential weapons on passengers who had passed security checkpoints have prompted evacuations at 124 airports and resulted in 631 flights being called back to terminals so that passengers could be searched again.

Furthermore, the enhanced security procedures have contributed to longer waits and congestion at airport terminals. TSA's goal is to process passengers through security in 10 minutes or less, but airlines have reported significantly longer waits during peak times at a number of the nation's major airports. These conditions can discourage air travel and adversely affect the travel industry.

Finally, the challenge of identifying and removing airport workers who cannot meet new requirements for background checks continues. Last October FAA ordered background checks on an estimated 750,000 airport and airline employees with access to secured areas of airports. By April 28, 2002, federal law enforcement officials had arrested or indicted more than 450 workers at 15 airports for being in the United States illegally or using phony social security numbers. These workers, who were employed by private companies that clean airplanes, operate airport restaurants, and provide other airport services, had security badges giving them access to planes, ramps, runways, and cargo areas. Completing these background checks will enhance aviation security.

Some other immediate challenges, such as the security of cargo and general aviation, were discussed in the act itself, and more recent legislative proposals

have raised these and other outstanding aviation security issues. To address these issues, bills have been introduced to arm pilots, enhance cargo security, require background checks for all foreign applicants to U.S. flight schools, prohibit the opening of cockpit doors during flights, train airline personnel to conduct passenger identification checks, make it a criminal penalty to intentionally circumvent airport security, and provide whistleblower protection for air carrier and airport security workers. (See app. III for a summary of pending legislation on aviation security.) All of these are complex and controversial issues. In moving forward, TSA must work with stakeholders to assess the risks and vulnerabilities of the various options and carefully weigh both the policy implications and the implementation strategies required for their success, keeping in mind the long-term implications of short-term decisions.

To illustrate the challenges and complexities TSA faces in attempting to strengthen aviation security, we examined some of the issues raised by proposals to arm pilots; establish a “trusted traveler” program, which would use biometric identifiers to expedite security checks; and enhance cargo security.

### Arming Pilots

Last month, at the request of this Committee’s Chairman, we provided information on, among other things, reasons for and against arming pilots and questions to be addressed if pilots were to be armed.<sup>5</sup>

- Proponents of arming pilots cited the potential deterrent value of firearms, their usefulness as a last line of defense, and past regulatory precedents, while opponents cited the moral dilemma pilots would face if they were prohibited from leaving the cockpit, as they would be by the legislation, when passengers or crew members were being threatened in the cabin. Opponents also said that arming pilots would introduce another 10,000 to

---

<sup>5</sup>Information Concerning the Arming of Commercial Pilots (GAO-02-822R, June 28, 2002).

100,000 guns into our society, which they believe would have negative effects.

- Questions to be addressed if pilots were to be armed included (1) who would regulate and oversee pilots' carriage of weapons; (2) what qualifications and training pilots would need to carry weapons; (3) what types of weapons would be carried and how they would be maintained, stored, and transported; (4) what aircraft modifications would be required; and (5) how much it would cost to arm pilots.

### Trusted Traveler

TSA has not yet completed its evaluation of the benefits and disadvantages of a trusted traveler program. Such a program, if successfully implemented, could reduce airport waits and speed security checks for passengers who voluntarily submit information about themselves and undergo background checks. It could also minimize the economic disruption caused by congestion at the terminal by allowing airline and TSA staff to focus more attention on lesser known passengers who could present greater security risks. However, such a program has the potential to increase the system's vulnerability by using reduced security measures for some passengers. If terrorists were to steal the identities of trusted travelers, the consequences could be particularly dire.

The trusted traveler concept presents many procedural questions that would need to be answered before a decision could be reached on implementing the program. Such questions include which passengers would be eligible to enroll, what information would be collected, how frequently their status would be updated, what entity would run the program, and what biometric identifiers would be used to positively identify the passengers.

## Aviation Cargo Security

Both the act and recent legislative proposals have raised the security of aviation cargo as an issue. The act requires that all cargo transported in all-cargo aircraft be screened as soon as practicable, but it is silent on how best to accomplish this screening. TSA has not announced how it plans to meet this requirement, in part because it has focused most of its efforts on meeting the deadlines for screening passenger bags. Two recent legislative proposals (S. 2668 and S. 2656) call for enhancing aviation cargo security by tightening the security of the “known shippers” system—the major system currently used to ensure aviation cargo security. The DOT Inspector General and others have identified gaps in this program, which allows shippers who meet DOT’s requirements to ship their cargo without inspection. The proposed legislation calls for investigating known shippers more thoroughly to ensure they are who they say they are, establishing a documentary “chain of custody” for all shipments, and inspecting a greater percentage of cargo than is currently done. These legislative proposals are intended to address the most difficult problem in ensuring cargo security—screening the vast amount of cargo without major disruptions in service—by increasing the level of scrutiny on shippers, middlemen, and recipients.

### **TSA Faces Longer-Term Institutional Challenges**

TSA faces several longer-term challenges as it organizes itself to protect the nation’s transportation system. These challenges include strategically managing its workforce, controlling costs, and sharing threat information.

### Strategic Human Capital Management Is Essential for Maximizing TSA’s Performance

A human capital strategy is critical for TSA, which may have a workforce as large as 70,000. To assist agencies in managing their human capital more strategically, GAO has developed a model of strategic human capital management that

identifies cornerstones and related critical success factors that agencies should apply and steps they can take.<sup>6</sup> 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 ongoing work for this Committee, we are reviewing aspects of TSA's implementation of results-oriented practices, such as human capital management. Today we would like to share some preliminary observations on TSA's progress in this area.

TSA's success in protecting the nation's transportation system depends in large part on its ability to recruit, train, and retain key people. Our prior work on aviation security identified problems with the training and retention of contract screeners. TSA has been charged with hiring and training a federal screener workforce and has encountered unexpected difficulty in doing so, especially in large metropolitan areas. For example, at Baltimore-Washington International Airport—the first of 429 airports to be staffed with federal passenger screeners—TSA's hiring of screeners was delayed because high percentages of applicants did not show up for or did not pass their pre-hiring assessment. Only about a third of the qualified applicants who were contacted to schedule an assessment reported for their assessment, and of those who reported, only about a third passed. If TSA experiences similar problems in trying to staff other airports, then the hiring challenge facing the agency is daunting.

A critical success factor in human capital management is to tailor human capital approaches to meet organizational needs by using the full range of tools and flexibilities available to an agency under current laws and regulations. The act allows TSA to use and modify the personnel system established by FAA, which is exempt from many federal personnel provisions. To meet its need for talented resources quickly, TSA officials told us that they made use of flexibilities such as temporary hiring authority, on-the-spot hiring authority, and the authority to use

---

<sup>6</sup>U.S. General Accounting Office, *A Model of Strategic Human Capital Management*, GAO-02-373SP

detailees from other agencies and executives on loan from the private sector. TSA is also basing its compensation system on FAA's pay banding approach, which allows the agency to hire employees anywhere within broad pay bands for their positions. For example, the pay band for screeners ranges from \$23,600 to \$35,400 (from about \$11 to \$17 per hour).<sup>7</sup> Pay banding is one approach that can support a more direct link between pay and an individual's knowledge, skills, and performance if an agency's performance management systems can support this link.

Another critical success factor is linking individual performance to organizational goals. The act requires TSA to establish a performance management system and performance agreements, with organizational and individual goals for employees, managers, and executives. TSA has made progress in setting up the performance management system. The agency has drafted but not approved an interim employee performance management system for the current fiscal year. The system lays out the processes and procedures for establishing performance agreements that include organizational and individual goals and objectives, measuring and monitoring performance, determining employees' development needs, and appraising and rewarding employees. Until the interim system is approved, TSA has implemented a temporary performance agreement for newly hired screeners and supervisory screeners. The temporary performance agreement contains a general description of duties and the manner in which the duties should be performed; it does not include specific individual and organizational goals. Finalizing a performance management system linked to organizational goals is critical to motivating and managing staff, ensuring the quality of screeners' performance, and, ultimately, restoring public confidence in air travel.

---

(Washington, D.C.: March 2002).

<sup>7</sup>Before TSA assumed responsibility for oversight of screening, contract screeners' pay was much lower, ranging, for example, from \$7 to \$10 per hour.

## Cost Controls and Contractor Oversight Are Critical for Ensuring TSA's Success

Federal organizations have a stewardship obligation to acquire goods and services at reasonable prices; expend federal tax dollars appropriately; ensure financial accountability to the President, Congress, and American people; and prevent waste, fraud, and abuse. Long-term attention to cost and accountability controls for acquisition and related business processes will be critical both to ensuring TSA's success and to maintaining its integrity and accountability. Such attention includes establishing cost control mechanisms and monitoring contractors' performance with respect to cost, schedule, and quality. This is particularly important because of TSA's large acquisition and personnel needs.

TSA oversees many large-dollar contracts; however, according to the DOT Inspector General, it could improve its controls over these contracts, which total \$3.1 billion in fiscal year 2002. For example, TSA initially budgeted \$2,500 per screener for background checks but was able to reduce this estimate to \$200 per screener after the Inspector General expressed concern. This change is projected to save the agency approximately \$95 million in fiscal year 2002 alone. According to the Inspector General, although TSA has made progress in addressing certain cost-related issues, it has not established an infrastructure that provides an effective span of control to monitor contractors' costs and performance.

Cost controls are also important in establishing employee compensation levels and controlling salaries. While pay banding can be used to ensure that salaries are commensurate with position duties, it should not be used to arbitrarily set salaries higher than comparable positions in other agencies. For example, TSA is hiring law enforcement officers from a number of other law enforcement agencies.

TSA's starting salary for most federal air marshals is \$36,400, which is supplemented by a 25-percent law enforcement pay differential that raises it to \$45,500. In contrast, the starting salaries for law enforcement employees at the Defense Protective Service, the U.S. Capitol Police, and the Federal Protective

Service--where some of the new federal air marshals previously worked--are capped at \$37,000, in part because they do not include this pay differential.

Further cost reductions due to efficiencies and economies of scale may be possible if TSA is moved to the proposed Department of Homeland Security. Costs reductions might be possible by consolidating administrative, technical, or other types of staff. As a result, TSA should exercise caution in staffing certain positions, such as creating its own criminal investigative workforce, when such functions might be merged with an already existing workforce. For example, under the President's proposal, Customs and the Immigration and Naturalization Service (INS), which have a combined criminal investigative workforce of about 5,000, would join TSA in reporting to an Under Secretary for Border and Transportation Security.

#### Information Sharing and Coordination Among Agencies Are Crucial for Threat Identification and Response

Timely, accurate information about terrorists and the threats they pose is vital to TSA's mission. Such information is gathered and maintained by numerous law enforcement and other agencies, including the Federal Bureau of Investigation (FBI), INS, the Central Intelligence Agency (CIA), and the State Department. Timely information sharing among such agencies has been hampered by organizational cultures that make agencies reluctant to share sensitive information and by outdated computer systems that lack interoperability. For example, INS, FBI, and the State Department all need the capacity to identify aliens in the United States who are in violation of their visa status, have broken U.S. laws, or are under investigation for criminal activity, including terrorism. In the immediate aftermath of September 11, it was reported that the computerized database systems of INS and State were incompatible, making data sharing difficult and cumbersome.

Increased coordination among agencies with responsibilities for national security is called for in the act, as well as in proposals for the creation of a new Department of Homeland Security. Specifically, the act established a transportation security oversight board, which is responsible for (1) facilitating the coordination of intelligence, security, and law enforcement activities affecting transportation; (2) facilitating the sharing of threat information affecting transportation among federal agencies and with airlines and other transportation providers; and (3) exploring the technical feasibility of developing a common database of individuals who may pose a threat to transportation or national security. The board includes representation from the DOT, CIA, National Security Council, Attorney General, the Departments of Defense and Treasury, and the Office of Homeland Security. Similarly, proposals to create a new Department of Homeland Security include provisions to share and coordinate intelligence information among many federal agencies. Moving TSA and agencies with responsibility for border protection, such as INS, into the proposed Department of Homeland Security may provide the opportunity for increased information sharing using state-of-the-art technology to manage threat information.

### **Closing Observations**

Mr. Chairman, it is worth repeating the two central issues confronting TSA as it strives to improve aviation security: it must meet mandated deadlines and demonstrate results swiftly while it creates a federal agency whose plans, policies, and procedures generally ensure long-term success. Achieving either goal would be challenge enough; to accomplish both simultaneously requires truly extraordinary efforts. Carefully considering how it strategically manages its large workforce, controls costs, and coordinates with other agencies to share threat information will help it meet its mission both now and in the future.

-----

This concludes my prepared statement. I will be pleased to answer any questions that you or Members of the Committee may have.

### **Contacts and Acknowledgments**

For more information, please contact Gerald L. Dillingham at (202) 512-2834. Individuals making key contributions to this testimony included Bonnie A. Beckett, Elizabeth Eisenstadt, Colin J. Fallon, David Goldstein, Samantha Goodman, David Hooper, Heather Krause, Bob Kolasky, Lisa Shames, Teresa Spisak, and Marti Tracy.

**Selected GAO Reports and Testimonies on Aviation Security**

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

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

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

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

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

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

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

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

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

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

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

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

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

## Appendix I

*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.

*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.

## Appendix I

*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-97-119R. 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.

Appendix I

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

**Deadlines in the Aviation and Transportation Security Act**

<b>Deadline</b>	<b>Provision<sup>a</sup></b>
Nov. 19, 2001	<p>Require new background checks for those who have access to secure areas of the airport</p> <p>Institute a 45-day waiting period for aliens seeking flight training for planes of 12,500 pounds or more</p>
Dec. 19, 2001	<p>Establish qualifications for federal screeners</p> <p>Report to The Congress on improving general aviation security</p>
Jan. 18, 2002	<p>Screen all checked baggage in U.S. airports using explosive detection systems, passenger-bag matching, manual searches, canine units, or other approved means</p> <p>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 training of all flight and cabin crews)</p> <p>Develop a plan to train federal screeners</p> <p>Foreign and domestic carriers are to provide electronic passenger and crew manifests to Customs for flights from foreign countries to the United States.</p> <p>Begin collecting the passenger security fee</p>
Feb. 17, 2002	<p>The Under Secretary is to assume civil aviation security functions from FAA</p> <p>Implement an aviation security program for charter carriers</p> <p>Begin awarding grants for security-related research and development</p> <p>The National Institute of Justice is to report to the Secretary on less-than-lethal weapons for flight crew members</p>
May 18, 2002	<p>Recommend commercially available security measures to airports for secure areas</p> <p>Report to The Congress on the deployment of baggage screening equipment</p> <p>Report to The Congress on progress in evaluating and taking the following optional actions:</p> <ul style="list-style-type: none"> <li>• Require 911 capability for onboard passenger telephones</li> <li>• Establish uniform IDs for law enforcement personnel carrying weapons on planes or in secure areas</li> <li>• Establish requirements for trusted traveler programs</li> <li>• Develop alternative security procedures to avoid damage to medical products</li> <li>• Provide for the use of secure communications technologies to inform airport security forces about passengers who are identified on security databases</li> <li>• Require pilot licenses to include a photograph and biometric identifiers</li> <li>• Use voice stress analysis, biometric, or other technologies to prevent high-risk passengers from boarding</li> <li>• Provide for the use of instant communications technology between planes and ground</li> </ul>

## Appendix II

<b>Deadline</b>	<b>Provision<sup>a</sup></b>
Nov. 19, 2002	<p>Deploy federal screeners, security managers, and law enforcement officers to screen passengers and property</p> <p>Report to The Congress on screening for small aircraft with 60 or fewer seats</p> <p>Establish pilot program to contract with private screening companies (program to last until Nov. 19, 2004)</p>
Dec. 31, 2002	Screen all checked baggage by explosive detection systems
May 18, 2003	Review reductions in secure-area incursions
No deadline	<p>Carriers are to transfer screening property to TSA</p> <p>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</p> <p>Improve perimeter screening of all individuals, goods, property, and vehicles</p> <p>Screen all cargo on passenger flights and cargo-only flights</p> <p>Establish procedures for notifying FAA, state and local law enforcement officers, and airport security of known threats</p> <p>Establish procedures for airlines to identify passengers who pose a potential security threat</p> <p>FAA is to develop and implement methods for using cabin video monitors, continuously operating transponders, and notifying flight deck crew of a hijacking</p> <p>Require flight training schools to conduct security awareness programs for employees</p> <p>Work with airport operators to strengthen access control points and consider deploying technology to improve security access</p> <p>Provide operational testing for screeners</p> <p>Assess dual-use items that seem harmless but could be dangerous and inform screening personnel</p> <p>Establish a system for measuring staff performance</p> <p>Establish management accountability for meeting performance goals</p> <p>Periodically review threats to civil aviation, including chemical and biological weapons</p>

<sup>a</sup>Provisions apply to TSA except where otherwise noted.

### Pending Legislation on Aviation Security

Bill number and date	Name/Subject	Key features
S. 1794 Dec. 10, 2001	Airport Checkpoint Enhancement Act	<ul style="list-style-type: none"> <li>• Subjects individuals who intentionally circumvent, in an unauthorized manner, a security system or procedure within a U.S. commercial service airport, to criminal penalties, including imprisonment for up to 10 years.</li> </ul>
S. 1980 Mar. 1, 2002	Training of Airline Personnel on Passenger Identification Checks	<ul style="list-style-type: none"> <li>• Directs the FAA Administrator and appropriate personnel, including TSA, to develop guidance within 60 days for training all commercial aviation personnel who are responsible for checking passenger identification.</li> <li>• Directs each air carrier to develop and submit a training program that meets these guidelines to the Administrator within 60 days. Also requires air carriers, within 180 days of receiving the Administrator's approval, to complete the training of all airline personnel responsible for checking passenger identification.</li> <li>• Directs the Administrator to establish and carry out a program to require the installation and use at airports within 180 days of identification verification technologies, such as identification scanners or retinal or facial scanners, to assist in the screening of passengers.</li> </ul>
S. 2497 May 9, 2002	Would prohibit opening of cockpit doors during flight	<ul style="list-style-type: none"> <li>• Requires that the door of any aircraft that is required to have a door between the passenger and pilot compartments remain closed and locked at all times during flight. Establishes a mantrap door exception that allows authorized persons to enter or leave the cockpit if the aircraft is equipped with double doors and remote cameras between the doors.</li> </ul>
S. 2554 May 23, 2002	Arming Pilots Against Terrorism and Cabin Defense Act	<ul style="list-style-type: none"> <li>• Establishes a program within 90 days to (1) deputize volunteer qualified pilots of commercial cargo or passenger aircraft as federal flight deck officers; and (2) provide training, supervision, and equipment for such officers.</li> <li>• Requires TSA to deputize at least 500 qualified pilots within 120 days. Requires full implementation within 2 years.</li> <li>• Authorizes flight deck officers to carry firearms and to use force, including lethal force, when they judge an aircraft's security at risk. Shields an air carrier from liability for the actions of the crew in defending an aircraft.</li> <li>• Directs the formation of the Aviation Crew Self-Defense Division within TSA.</li> </ul>
S. 2642 June 18, 2002	Would require background checks for alien flight school applicants	<ul style="list-style-type: none"> <li>• Eliminates the current background check requirement for aliens taking training at flight schools, which applies only to training on planes that weigh 12,500 pounds or more.</li> <li>• Requires background checks for all alien flight school applicants regardless of the size of the plane that would be used in their training.</li> <li>• Requires the Transportation and Justice departments to report to The Congress within 1 year on the effectiveness of the program.</li> </ul>
S. 2656 June 20, 2002	Would establish cargo security measures	<ul style="list-style-type: none"> <li>• Requires the head of TSA to submit to the Congress by Sept. 30, 2002, a security plan for the transportation of cargo into and out of the United States and to oversee the implementation of security measures with respect to cargo at airports and other transportation facilities. The final plan must be implemented by Sept. 30, 2003.</li> <li>• By that date, the head of TSA must implement random screening of at least 5 percent of cargo at airports and other transportation facilities, an authentication policy for "known shippers," regular audits of shippers to ensure full compliance with security procedures and background check requirements for cargo handlers, and develop a security training program for entities that handle cargo.</li> </ul>

Appendix III

Bill number and date	Name/Subject	Key features
S. 2668 June 21, 2002	Air Cargo Security Act	<ul style="list-style-type: none"> <li>• Requires the head of TSA to establish a security system to screen cargo in all passenger and cargo aircraft. Further requires the head of TSA to ensure that this security system establishes a verifiable record of the chain of custody for cargo and that each person who handles the cargo is known and properly certified.</li> <li>• Requires the establishment of a comprehensive system of certification for shippers and providers of cargo transportation services that includes the assignment of a unique encrypted identifier, as well as a system for the regular inspection of shipping facilities for cargo.</li> </ul>
S. 2686 June 26, 2002	Airport Employee Whistleblower Protection Act	<ul style="list-style-type: none"> <li>• Establishes whistleblower protection for employees of air carriers or contractors or subcontractors of air carriers and airport security personnel, both federal and local.</li> </ul>
S. 2735 IS July 16, 2002	Aviation Security Enhancement Act (Same exact legislation as the House bill of the same name.)	<ul style="list-style-type: none"> <li>• Requires the Under Secretary to notify individual airports of the number and type of explosive detection systems (EDS) to be deployed by Oct. 1, 2002.</li> <li>• Requires airports to notify TSA by Nov. 1, 2002, if they will be unable to meet those requirements by Dec. 31, 2002. If so, requires TSA and the airports to work together to develop an alternative plan.</li> <li>• If EDSs are not in place at a U.S. airport on Dec. 31, 2002, allows alternative methods, such as hand searches and bag matching, until the EDSs are in place.</li> <li>• Requires all EDSs to be placed in nonpublic areas to the maximum extent practicable.</li> <li>• Requires that TSA purchase any EDSs on behalf of the airports.</li> <li>• Requires that TSA conduct demonstration projects of alternatives to EDSs. TSA shall report the results of these projects to The Congress by Dec. 31, 2003.</li> </ul>
H.R. 4635 May 1, 2002	Arming Pilots Against Terrorism Act	<ul style="list-style-type: none"> <li>• Directs TSA to establish a program to (1) deputize volunteer pilots of air carriers as federal law enforcement officers to defend the flight decks of aircraft against acts of criminal violence or air piracy and (2) provide training, supervision, and equipment for such officers.</li> <li>• Requires the Under Secretary to begin training and deputizing qualified pilots to be federal flight deck officers under the program.</li> <li>• Directs TSA to authorize flight deck officers to carry firearms and to use force, including lethal force, according to standards and circumstances the Under Secretary prescribes. Precludes an air carrier from prohibiting or threatening any retaliatory action against a pilot for becoming a federal flight deck officer.</li> <li>• Amends the Aviation and Transportation Security Act to authorize the Under Secretary to take certain enhanced security measures, including to require that air carriers provide flight attendants with a discreet, hands-free, wireless method of communicating with the pilot of an aircraft.</li> <li>• Directs the Under Secretary to study and report to the Congress on the benefits and risks of providing flight attendants with nonlethal weapons to aid in combating air piracy and criminal violence on commercial airlines.</li> </ul>

### Appendix III

Bill number and date	Name/Subject	Key features
H.R. 5005 June 24, 2002	Homeland Security Act of 2002	<ul style="list-style-type: none"> <li>• Requires TSA to consult with FAA before taking any action that might affect aviation safety, air carrier operations, aircraft airworthiness, or the use of airspace.</li> <li>• Maintains TSA as a distinct entity within the Department of Homeland Security. Provides that TSA will cease to exist as a distinct entity after 2 years.</li> <li>• Requires TSA to notify all major airports by Oct. 1, 2002, of the number and type of EDSs that they will be required to deploy in order to screen all checked baggage by Dec. 31, 2002. Allows the airports to use other methods of screening, such as bag matching, canine sniffers, or other technology, if they cannot make the modifications necessary to meet the Dec. 31, 2002, deadline.</li> <li>• Requires that the total number of passengers and baggage screeners in place after Nov. 19, 2002, shall not be less than were deployed on Sept. 11, 2001, at each individual airport.</li> </ul>

(540034)