United States General Accounting Office

GAO

Testimony

Before the National Commission on Terrorist Attacks Upon the United States

For Release on Delivery
Expected at 10:30 a.m. EST
in New York, New York
Tuesday, April 1, 2003

TRANSPORTATION SECURITY

Post-September 11th Initiatives and Long-Term Challenges

Statement of Gerald L. Dillingham
Director, Physical Infrastructure Issues

GAO-03-616T

March 31, 2003

TRANSPORTATION SECURITY

Post-September 11th Initiatives and Long-Term Challenges

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-616T, a testimony before the National Commission on Terrorist Attacks Upon the United States

Why GAO Did This Study

This testimony responds to the request of the National Commission on Terrorist Attacks Upon the United States for information on GAO's work in transportation security. It addresses (1) transportation security before September 2001; (2) what the federal government has done since September 11th to strengthen transportation security, particularly aviation, mass transit, and port security; and (3) what long-term institutional challenges face the federal agencies responsible for transportation security. The testimony is based on a body of work that GAO has performed over the years.

What GAO Recommends

This testimony does not contain recommendations. However, GAO reports and testimonies on aviation, transit, and port security and on management issues are listed at the end of the statement. Many of these reports and testimonies contain GAO recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-03-616T

To view the full report, 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

Before September 2001, GAO's work in transportation security focused largely on aviation security, which was then the responsibility of the Federal Aviation Administration, within the Department of Transportation. This work often demonstrated the existence of significant, long-standing vulnerabilities in aviation security. Among these vulnerabilities were airport screeners' inadequate detection of threats when screening passengers and their carry-on bags prior to their boarding aircraft; the absence of any requirement to screen checked baggage on domestic flights; inadequate controls for limiting access to secure areas at airports; and inadequate security for air traffic control computer systems and facilities.

Since September 2001, securing the nation's transportation systems from terrorist attacks has assumed great urgency. The Congress and the administration have reorganized the federal agencies responsible for transportation security, transferring them to the new Department of Homeland Security, and the agencies are attempting to enhance security without unduly inhibiting the movement of goods and people. The Transportation Security Administration, which was created in November 2001 and has assumed overall responsibility for transportation security, has made considerable progress in addressing aviation security challenges. By the end of December 2002, the agency had hired and deployed a workforce of over 60,000, including passenger and baggage screeners and federal air marshals, and was screening about 90 percent of all checked baggage for explosives. In addition, local mass transit agencies have assessed vulnerabilities, increased training for emergency preparedness, and conducted emergency drills. The Coast Guard has also performed initial risk assessments of ports, established new security guidelines, and initiated a comprehensive assessment of security conditions at 55 U.S. ports. The Customs Service and the Immigration and Naturalization Service have actions under way to strengthen port security. Nevertheless, air cargo shipments, general aviation airports, and mass transit systems remain vulnerable to attack, and an effective port security environment may be many years away.

The Departments of Transportation and Homeland Security face long-term transportation security challenges that include (1) developing a comprehensive transportation risk management approach; (2) ensuring that transportation security funding needs are identified and prioritized and that costs are controlled; (3) establishing effective coordination among the many public and private entities responsible for transportation security; (4) ensuring adequate workforce competence and staffing levels; and (5) implementing security standards for transportation facilities, workers, and security equipment. We have issued reports and made recommendations that address many of these challenges, and in response some actions are under way.

Mr. Chairman and Members of the Commission:[1]

We are here today to discuss our public work on transportation security. As you know, the General Accounting Office is the audit, evaluation, and investigative arm of the Congress. Our mission is to support the Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. We examine the use of public funds; evaluate federal programs and policies; and provide analyses, recommendations, and other assistance to help the Congress make informed oversight, policy, and funding decisions. Our commitment to good government is reflected in our core values of accountability, integrity, and reliability. We wish to thank the Commission for inviting us today to share our knowledge of transportation security issues, and we look forward to continuing to work with you.

Since September 11, 2001, securing our nation's transportation system from terrorist attacks has assumed great urgency. On November 19, 2001, the Congress enacted the Aviation and Transportation Security Act, which created the Transportation Security Administration (TSA) within the Department of Transportation (DOT) and defined its primary responsibility as ensuring security in all modes of transportation. DOT then worked to strengthen security through its modal administrations while simultaneously organizing the new agency to meet the longer-term challenge of implementing security improvements that will not excessively inhibit commerce and travel or interfere with other critical agency missions. With the passage of the Homeland Security Act on November 25, 2002, TSA was transferred to the new Department of Homeland Security, which assumed overall responsibility for transportation security.

My testimony today addresses (1) transportation security before September 2001; (2) what the federal government has done since September 11th to strengthen transportation security, particularly aviation, mass transit, and port security; and (3) the long-term institutional challenges that face the federal agencies responsible for transportation security.

[1]The National Commission on Terrorist Attacks Upon the United States is an independent, bipartisan commission created by Public Law 107-306 to investigate the circumstances surrounding the events of September 11, 2001, and make recommendations for corrective measures that can be taken to prevent acts of terrorism.

In summary:

Before September 2001, our work in transportation security focused largely on aviation security, which was then the responsibility of DOT's Federal Aviation Administration (FAA). Together with other studies, our work often demonstrated the existence of significant, long-standing vulnerabilities in aviation security. These vulnerabilities included failure to detect threats when screening passengers and their carry-on bags prior to their boarding aircraft and the absence of any requirement to screen checked baggage on domestic flights; inadequate controls for limiting access to secure areas at airports; and failure to secure air traffic control computer systems and facilities.

Since September 2001, securing our nation's transportation system from terrorist attacks has assumed great urgency. The Congress and the administration have reorganized the federal agencies responsible for transportation security, transferring them to the new Department of Homeland Security, and the agencies are attempting to enhance security without unduly inhibiting the movement of goods and people. TSA has made considerable progress in addressing aviation security challenges. By the end of December 2002, the agency had hired and deployed a workforce of over 60,000, including passenger and baggage screeners and federal air marshals, and was screening about 90 percent of all checked baggage for explosives. In addition, local mass transit agencies have assessed vulnerabilities, increased training for emergency preparedness, and conducted emergency drills. The Coast Guard has also performed initial risk assessments of ports, established new security guidelines, and initiated a comprehensive assessment of security conditions at 55 U.S. ports, and the Customs Service and the Immigration and Naturalization Service have actions under way to strengthen port security. Nevertheless, air cargo shipments, general aviation airports, and mass transit systems remain vulnerable to attack, and an effective port security environment may be many years away.

DOT and the Department of Homeland Security face long-term transportation security challenges that include (1) developing a comprehensive risk-management approach; (2) ensuring that transportation security funding needs are identified and prioritized and that costs are controlled; (3) establishing effective coordination among the many public and private entities responsible for transportation security; (4) ensuring adequate workforce competence and staffing levels; and (5) implementing security standards for transportation facilities, workers, and

security equipment. We have issued reports and made recommendations that address many of these challenges, and some actions are under way.

Some Vulnerabilities in Transportation Security Were Known before September 2001

Our work on transportation security prior to September 2001 primarily addressed vulnerabilities in aviation security. These included ineffective screening of passengers and baggage for threat objects and explosives, inadequate controls for limiting access to secure areas at airports, and inadequate security for air traffic control computer systems and facilities. Mass transit agencies were taking actions to enhance security, and concerns about port security were raised.

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. As we reported in June 2000, tests of screeners conducted in 1987 revealed that screeners missed 20 percent of the potentially dangerous objects that FAA used in its tests, and test data from 1991 through 1999 showed a declining trend in the rate of detection.[2] At that time, FAA characterized this level of performance as unsatisfactory. The more recent results showed that as testing got more realistic—that is, as tests more closely approximated how a terrorist might attempt to penetrate a checkpoint—screeners' performance declined significantly. A principal cause of screeners' performance problems was rapid turnover and insufficient training. Turnover exceeded over 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.

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.[3] 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

[2]U.S. General Accounting Office, *Aviation Security: Long-Standing Problems Impair Airport Screeners' Performance*, GAO/RCED-00-74 (Washington, D.C.: June 28, 2000).

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

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.

Before September 2001, our reviews of FAA's oversight of air traffic control computer systems showed that FAA had not ensured the security of these systems or of the facilities that house them.[4] Our reviews also found that FAA had not ensured that the contractors who had access to the air traffic control computer systems had undergone background checks. 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 a loss of life because of collisions. Because of the vulnerabilities we identified, the air traffic control system was susceptible to intrusion and malicious attacks.

Over the years, we made numerous recommendations to FAA 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.

Before September 2001, many transit agencies were implementing measures to enhance transit safety and security, such as revising emergency plans and training employees in emergency preparedness. According to transit agency officials, the 1995 sarin gas attack on the Tokyo subway system and experiences during natural disasters had served as catalysts for the agencies to focus on safety and security. The officials said that the terrorist attacks on September 11th elevated the importance of security.

[4] *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).

Concerns about the security of the nation's ports were recognized even before the September 11th attacks. Ports are inherently vulnerable to terrorist attacks and make desirable targets because of their size, accessibility by water and land, location in metropolitan areas, volume of material transported, and ready transportation links to interior locations. Moreover, a terrorist act at one of these seaports could result in extensive loss of lives, property, and business, and could impact the nation's economy if the free flow of trade is disrupted. In August 2000, the Interagency Commission on Crime and Security in U.S. Seaports estimated that the costs to upgrade the security infrastructure at the nation's 361 ports ranged from $10 million to $50 million per port.

Since September 2001, Federal Agencies Have Put People, Policies, and Procedures in Place to Strengthen Transportation Security

Since September 2001, federal and local agencies have been trying to assess and address the monumental challenges they face in attempting to strengthen the security of the nation's transportation systems. As we testified on September 20, 2001, the enormous size of the U.S. airspace alone defies easy protection, and no form of travel can ever be made totally secure. Providing aviation security means protecting hundreds of airports, thousands of planes, and tens of thousands of daily flights. Providing transit and port security also poses daunting challenges. For example, about 6,000 agencies provide transit services through buses, subways, ferries, and light rail service to about 14 million Americans each weekday, and millions of containers are imported into the United States through more than 300 public and private U.S. seaports, with more than 3,700 cargo and passenger terminals.

The federal government's role in transportation security has been evolving since September 2001. TSA was created in November 2001 by the Aviation and Transportation Security Act and has assumed overall responsibility for transportation security. Although the agency has thus far focused primarily on aviation, it is responsible under the act for the security of all modes of transportation, which also include mass transit, maritime, rail, highway, and pipelines. TSA is in the early stages of working with the other transportation modes. We highlight some of the progress that has been made in aviation, mass transit, and port security.

Aviation Security

Following the September 11th attacks, DOT faced several urgent aviation security challenges, such as meeting newly established screening deadlines and addressing security gaps that we and others, including DOT's Inspector General, had identified. In November 2001, TSA assumed responsibility under the Aviation and Transportation Security Act for

screening passengers and property. (See fig. 1.) The act required it to hire and deploy federal passenger screeners by November 19, 2002, and to screen all checked baggage using explosives detection systems by December 31, 2002.[5] In addition, FAA established a requirement for installing reinforced cockpit doors in aircraft.

[5]The Homeland Security Act of 2002 amends this requirement. According to the legislation, if, in his discretion or at the request of an airport, the Under Secretary of Transportation for Security determines that TSA is not able to deploy the explosives detection systems required in the Aviation and Transportation Security Act by December 31, 2002, then for each airport for which the Under Secretary makes this determination, the Under Secretary shall submit to specific congressional committees a detailed plan for the deployment of the number of explosives detection systems at that airport necessary to meet the requirements as soon as practicable at that airport but no later than December 31, 2003; the Under Secretary shall take all necessary action to ensure that alternative means of screening all checked baggage are implemented until the requirements have been met.

Figure 1: Passengers Being Screened at a Security Checkpoint

Source: FAA.

TSA has made considerable progress in addressing aviation security challenges. For example, according to TSA, it

- met the November 2002 deadline by hiring and deploying over 40,000 passenger screeners to screen passengers at 429 commercial airports;
- hired and deployed more than 20,000 of an estimated 22,000 baggage screeners as of mid-December 2002 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;[6]

[6]Explosives detection machines are used to screen baggage for explosives and work by using CAT scan X-ray 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.

- has been using alternative means such as canine teams, hand searches, and passenger-bag matching to screen the remaining checked baggage; and
- has made substantial progress in expanding the Federal Air Marshal Service.

Furthermore, according to an FAA official, as of March 21, 2003, FAA had approved designs for reinforcing the cockpit doors of over 98 percent of the commercial fleet's 5,750 aircraft, 80 percent of the doors had been installed, and kits had been ordered for the remaining doors. As of mid-December 2002, however, TSA still had to complete the installation of most of the explosives detection equipment needed to screen baggage to meet the act's baggage-screening requirements. At that time, according to TSA, it had installed 239 of the 1,100 explosives detection machines and 1,951 of the 6,000 trace detection machines that it had estimated were needed.

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 exist in securing the cargo carried aboard commercial passenger and all-cargo aircraft. The Aviation and Transportation Security Act 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. The "known shipper" program—which allows shippers that have established business histories with air carriers or freight forwarders[7] to ship cargo on planes—is TSA's primary approach to ensuring air cargo security and safety and to complying with the cargo-screening requirement of the act. However, we and DOT's Inspector General have identified weaknesses in the known shipper program and in TSA's procedures for approving freight forwarders.[8]

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

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

[8]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).

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.[9] 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.[10] Accordingly, we recommended that TSA develop a comprehensive plan for air cargo security that incorporates a risk management approach, includes a list of security priorities, and sets deadlines for completing actions. TSA agreed with this recommendation.

Since September 2001, TSA has taken only a few actions related to general aviation security, leaving it far more open and potentially vulnerable than commercial aviation. 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. General aviation's vulnerability was revealed in January 2002, when a Florida teenager (and flight student) crashed a single-engine Cessna airplane into a Tampa skyscraper. FAA has since issued a notice with voluntary guidance for flight schools that suggests such measures as 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 reporting suspicious activities. However, because the guidance is voluntary, it is unknown how many flight schools have implemented these measures.

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. However, more must be done to ensure that critical information systems are not at risk of intrusion and attack. Among its accomplishments, 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, 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

[9]GAO-03-344.

[10]GAO-03-344.

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 agency policy. Finally, FAA has worked aggressively over the past 2 years to complete background investigations on 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.

Mass Transit

Transit agencies face significant challenges in making their systems secure, in part because certain characteristics that make them vulnerable also make them difficult to secure. For example, the high ridership of some transit agencies makes them attractive targets for terrorists but also makes the use of certain security measures, like metal detectors, impractical. Despite such challenges, transit agencies have taken a number of steps to improve the security of their systems. In December 2002, after visiting 10 transit agencies and surveying 200, we reported that these agencies had implemented new security initiatives or increased the frequency of existing activities since September 2001.[11] For example, many transit agencies had assessed vulnerabilities, provided additional training on emergency preparedness, revised emergency plans, and conducted multiple emergency drills. (See fig. 2.) Several agencies we visited had also implemented innovative practices to enhance safety and security, such as training police officers to drive buses and implementing an employee suggestion program to solicit ideas for improving security.

[11]U.S. General Accounting Office, *Mass Transit: Federal Action Could Help Transit Agencies Address Security Challenges*, GAO-03-263 (Washington, D.C.: Dec. 13, 2002).

Figure 2: Emergency Transit Drill in Progress

Source: GAO

At a planned emergency drill, firefighters practice rescuing passengers from a Washington Metropolitan Area Transit Authority subway car.

After September 2001, the Federal Transit Administration (FTA), which has limited authority to oversee and regulate transit security, launched a multipart security initiative. Although most of the transit agencies we visited said this initiative was useful, they wanted the federal government to provide more assistance to support transit security, such as more information, help in obtaining security clearances, increased funding, and more security-related research and development. To give transit agencies greater flexibility in paying for transit security improvements, we recommended that the Secretary of Transportation consider seeking a legislative change to allow all transit agencies, regardless of the size of the

urbanized area they serve, to use urbanized area formula funds[12] for security-related operating expenses. We also recommended that the Secretary of Transportation develop risk-based criteria for distributing federal funds to transit agencies for high-priority security improvements. The department agreed to carefully consider our recommendations as it continues working to improve transit security around the country.[13]

Port Security

Since September 2001, federal agencies, state and local authorities, and private-sector stakeholders have done much to address vulnerabilities in the security of the nation's ports.[14] The Coast Guard, in particular, has acted as a focal point for assessing and addressing security concerns. After September 11th, the Coast Guard responded by refocusing its efforts and repositioning vessels, aircraft, and personnel not only to provide security, but also to increase visibility in key maritime locations. Some of its actions included (1) conducting initial risk assessments of ports, which identified high-risk infrastructure and facilities and helped determine how the Coast Guard's small boats would be used for harbor security patrols; (2) initiating new guidelines for developing security plans and implementing security measures for passenger vessels and passenger terminals; and (3) beginning a process to comprehensively assess the security conditions of 55 U.S. ports over a 3-year period.

In addition, shortly after September 11th, the Coast Guard began requiring ships to provide earlier notification of their scheduled arrival at a U.S. port. All vessels over 300 gross tons are now required to contact the Coast Guard 96 hours—up from 24 hours—before they are scheduled to arrive at a U.S. port. Each vessel must provide information on its destination, its scheduled arrival, the cargo it is carrying, and a roster of its crew members. The information, which is processed and reviewed by the Coast Guard's National Vessel Movement Center, is used in conjunction with data from various intelligence agencies to identify "high-interest" vessels. Decisions on appropriate actions to be taken with respect to such vessels,

[12]The federal urbanized area formula program provides federal funds to urbanized areas (jurisdictions with populations of 50,000 or more) for transit capital investments, operating expenses, and transportation-related planning.

[13]We are currently examining TSA's role in the security of transit and all other modes of transportation. We expect to report on this work later this spring.

[14]U.S. General Accounting Office, *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful*, GAO-02-993T (Washington, D.C.: Aug. 5, 2002).

such as whether to board, escort, or deny entry to them, are based on established criteria and procedures.[15] (See fig. 3.)

Figure 3: Inspecting Millions of Containers That Arrive at U.S. Ports Remains a Challenge

Source: © 1995 Noval Development Corporation.

Two other key federal agencies—the Customs Service and the Immigration and Naturalization Service—also have actions under way to begin to address such issues as container security and the screening of persons seeking entry into the United States. With more than 6 million containers a year entering U.S. ports, examining them all has not been possible. Using a targeted approach, Customs physically inspects about 2 percent of the containers that enter the country. New initiatives by the

[15]U.S. General Accounting Office, *Container Security: Current Efforts to Detect Nuclear Materials, New Initiatives, and Challenges*, GAO-03-297T (Washington, D.C.: Nov. 18, 2002).

Customs Service would widen inspection coverage. For example, the Customs Service's Container Security Initiative focuses on placing U.S. Customs inspectors at the ports of embarkation to target containers for inspection; the Customs Trade Partnership against Terrorism focuses on efforts by importers and others to enhance security procedures along their supply chain; and Operation Safe Commerce focuses on using new technology, such as container seals, to help shippers ensure the integrity of the cargo included in containers being sent to the United States.

Transportation Security Poses Long-Term Institutional Challenges

Efforts to strengthen transportation security face several long-term institutional challenges that include (1) developing a comprehensive risk management approach; (2) ensuring that funding needs are identified and prioritized and that costs are controlled; (3) establishing effective coordination among the many responsible public and private entities; (4) ensuring adequate workforce competence and staffing levels; and (5) implementing security standards for transportation facilities, workers, and security equipment.

Risk Management

To achieve transportation security as well as homeland security, it will be important to effectively manage the risks posed by terrorist threats and to direct national resources to the areas of highest priority. We have advocated the use of a risk management approach to guide federal programs and responses to better prepare for and withstand terrorist threats.[16] 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. Figure 4 describes this approach.

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

Figure 4: 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 decision making 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 to target resources to the highest priorities, while reducing the potential for targeting resources to lower priorities.

Source: GAO.

Our work has shown that TSA and some of DOT's modal administrations have partially developed risk management approaches. For example, in the fall of 2001, FAA completed an assessment of the threats to and vulnerabilities of air cargo. The assessment examined a single scenario—a terrorist attempting to place a bomb on a commercial passenger aircraft—but did not address the shipment's vulnerability to tampering along the route from the shipper to the aircraft. In December 2002, we also reported that FTA obtains threat information from a variety of sources, including the Federal Bureau of Investigation, and had started to identify the most critical transit infrastructure. Moreover, according to agency officials and our survey results, many transit agencies are conducting vulnerability or security assessments. Finally, as noted, the Coast Guard has already conducted initial risk assessments of the nation's ports, has established new security guidelines, and is planning for comprehensive assessments of security conditions at 55 U.S. ports. We have recommended that TSA conduct a comprehensive plan for air cargo security that incorporates a risk management approach, and we have recommended that FTA use a risk-based approach in prioritizing funding decisions for security projects. Both TSA and FTA agreed with our recommendations. Comprehensive risk-based assessments are important for all the modes, and they support effective planning and resource allocation.

Funding

Two key funding and accountability challenges will be (1) paying for increased transportation security and (2) ensuring that these costs are controlled. The costs associated with acquiring equipment and personnel for improving aviation security alone are huge. Although TSA estimates that it will need about $4.8 billion for aviation security in fiscal year 2003, it estimates that revenues from the new passenger security fee will pay for only around one-third ($1.7 billion) of that amount. As a result, TSA will need a major cash infusion at a time when federal budget deficits are growing. Similarly, many of the planned security improvements for surface transportation facilities, such as seaports and mass transit, require costly outlays for infrastructure, technology, and personnel at a time when weakening local economies have reduced local transportation agencies' abilities to fund security improvements.

Estimates of the funding needed to pay for port security far outstrip the amounts made available to date.[17] As we reported in August 2002, the Congress appropriated $93 million to fund security improvements at the nation's 361 ports in fiscal year 2002, but TSA received applications for as much as $697 million for these improvements. Efforts by the Coast Guard to develop security standards for ports, which we reported in August 2002, should help to identify and prioritize needs so that limited funds can be targeted to the highest risks at each port. Additional funding will be needed to comply with provisions of the Maritime Transportation Security Act, enacted in November 2002, which require, among other things, that regulations be developed for the preparation and submission of vessel and facility security plans, and that vulnerability assessments be conducted for vessels and U.S. port facilities.

In July 2002, we reported that 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.[18] 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. To ensure control over TSA contracts, DOT's Inspector General has recommended that the Congress set aside a

[17] GAO-02-993T.

[18] 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).

specific amount of TSA's contracting budget for overseeing contractors' performance with respect to cost, schedule, and quality.[19]

In considering the federal government's role in meeting long-term funding challenges, several issues will need to be addressed beyond determining who should pay for the security enhancements and to what extent the agency functions should be funded. An important consideration is, which criteria are most appropriate for distributing federal funds? The chief criteria considered have been ridership level, population, identified vulnerabilities, and criticality of assets. Another important consideration, as we reported in September 2002, is, which federal policy instruments—grants, loan guarantees, tax incentives, or partnerships—are most appropriate to motivate or mandate other levels of government or the private sector to help address security concerns?[20] Finally, it will be important to consider how to allocate funds between competing needs and to measure whether we are achieving the increased security benefits envisioned.

Coordination

Since September 2001, federal, state, and local surface transportation agencies and the private sector have begun rethinking roles and responsibilities for transportation security. One challenge to achieving national preparedness hinges on the federal government's ability to form effective partnerships among entities that implement security measures at the local level. Effective, well-coordinated partnerships require identifying roles and responsibilities; developing effective, collaborative relationships with local and regional transportation, emergency management, and law enforcement agencies; agreeing on performance-based standards that describe desired outcomes; testing procedures that implement roles and responsibilities; and sharing intelligence information.

Although TSA has focused primarily on aviation security challenges since its creation in 2001, it is working toward defining the roles and responsibilities for other modes. TSA has developed a memorandum of agreement with FAA that laid out general principles of cooperation and

[19]U.S. Department of Transportation, Office of Inspector General, *Key Challenges Facing the Transportation Security Administration*, CC-2002-180 (Washington, D.C.: June 20, 2002).

[20]U.S. General Accounting Office, *Mass Transit: Challenges in Securing Transit Systems*, GAO-02-1075T (Washington, D.C.: Sept. 18, 2002).

consultation between the two agencies. DOT and TSA expect that agreement to also serve as a guide to relations between TSA and DOT's other modal administrations.

Coordination challenges will continue now that TSA has been transferred to the new Department of Homeland Security. TSA will act as a national transportation system security manager and expects to work closely with DOT to establish security standards for all modes of transportation (air, mass transit, maritime, rail, highway, and pipelines). Both TSA and DOT will have to ensure the development of sound security policies and procedures and the effective implementation of those procedures by the many public and private transportation systems' stakeholders.

TSA will also have 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. In aviation security, timely information-sharing among agencies has been hampered by organizational cultures reluctant to share sensitive information and by outdated, incompatible computer systems. In surface transportation, timely information-sharing has been hampered by the lack of standard protocols to exchange information among federal, state, and local government agencies and private entities. Finally, as we reported in September 2002, intelligence-sharing can be hampered if personnel in surface transportation agencies have difficulty in acquiring the security clearances needed to obtain critical intelligence information.[21]

Human Capital

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. 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.[22] Our model is designed to help agency

[21]GAO-02-1075T.

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

leaders effectively lead and manage their people and integrate human capital considerations into daily decisionmaking and the program results they seek to achieve. In January 2003, we reported that TSA is 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.[23] However, concerns remain about TSA's approach to compensation and progress in setting up a performance management system. For example, DOT's Inspector General expressed concern about TSA's approach to compensation. TSA is 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. Last summer, the Inspector General reported that TSA's salary levels for law enforcement and general and administrative positions were higher than for comparable positions in other agencies. [24] TSA was also behind schedule in establishing a performance management system linked to organizational goals. Such a system will be critical in order for TSA to motivate and manage staff, ensure the quality of screeners' performance, and, ultimately, restore public confidence in air travel.

Security Standards for Surface Transportation

Security standards for transportation facilities, workers, and security equipment define the level of security that is needed and the safeguards that should be in place to meet identified security needs. Adequate standards, consistently applied, are important to ensure that operators improve their security practices in modes where lax security could make surface transportation facilities attractive targets for terrorists. New security standards are being developed in some modes and are being considered in other modes. For example, new security standards are being developed for ports, to prevent unauthorized persons from gaining access to sensitive areas, to detect and intercept intrusions, to check the backgrounds of those whose jobs require access to port facilities, and to screen travelers and other visitors to port facilities. The Maritime Transportation Security Act of 2002, enacted November 25, 2002, requires the development of (1) port security regulations for access controls, background checks, and vessel and facility security plans and (2)

[23]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).

[24]U.S. Department of Transportation, Office of Inspector General, *Progress in Implementing Provisions of the Aviation and Transportation Security Act*, CC-2002-203 (Washington, D.C.: Aug. 7, 2002).

performance standards for seals and locks on shipping containers. In addition, legislation proposed in the last session of Congress would require DOT to prescribe standards for pipeline security programs and to approve or disapprove each pipeline operator's program on the basis of the operator's adherence to these standards.[25] However, industry representatives have told us that they would prefer a nonregulatory approach, citing concerns about the need for flexibility in designing security programs suitable for each pipeline facility.

While progress has been made in developing security standards, challenges remain in implementing them. There is little precedent for how to enforce standards, because the size, complexity, and diversity of surface transportation facilities do not lend themselves to an enforcement approach similar to the one adopted for airports after September 11th. Implementing standards is also difficult because it requires consensus and compromises on the part of stakeholders. To the degree that some stakeholders believe that security actions are unnecessary or conflict with other goals and interests, achieving consensus about what to do will be difficult.

Concluding Observations

Where do we stand today? How much more secure are we now than we were before September 11th? After spending billions of dollars on people, policies, and procedures to improve security, we are much more secure now than we were then, but we can never be completely secure. Today, we have better intelligence, coordination, and communication; we have plans to alert the public to threats; and we are all more alert to the possibility of threats. Yet major vulnerabilities remain, particularly in air cargo, general aviation, mass transit, and port security. Addressing these vulnerabilities will continue to require risk assessments and plans that balance security concerns against mobility needs, and that consider how much the nation can afford to spend for security improvements in light of other, competing demands for limited funds.

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

[25]Pipeline Infrastructure Protection to Enhance Security and Safety Act, H.R. 3609, 107th Congress (2001).

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, Maren McAvoy, John W. Shumann, and Teresa Spisak.

Related GAO Products

Aviation Security

Aviation Security: FAA Needs to Update Curriculum and Certification Requirements for Aviation Mechanics. GAO-03-317. Washington, D.C.: March 6, 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 Safety: Undeclared Air Shipments of Dangerous Goods and DOT's Enforcement Approach. GAO-03-22. Washington, D.C.: January 10, 2003.

Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System. GAO-03-286NI. 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 Safety: Better Guidance and Training Needed on Providing Files on Pilots' Background Information. GAO-02-722. August 30, 2002.

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

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

*Aviation Security: Deployment and Capabilities of Explosive Detection Equipmen*t. 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. GAO/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.

Transit Security

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

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

Maritime Security

Coast Guard: Comprehensive Blueprint Needed to Balance and Monitor Resource Use and Measure Performance for All Missions. GAO-03-544T. Washington, D.C.: March 12, 2003.

Homeland Security: Challenges Facing the Coast Guard as It Transitions to the New Department. GAO-03-467T. Washington, D.C.: February 12, 2003.

Container Security: Current Efforts to Detect Nuclear Materials, New Initiatives, and Challenges. GAO-03-297T. Washington, D.C.: November 18, 2002.

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

Other

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.