United States General Accounting Office

GAO

Testimony

Before the Committee on Commerce, Science, and Transportation United States Senate

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

TRANSPORTATION SECURITY

Federal Action Needed to Enhance Security Efforts

Statement of Peter Guerrero, Director
Physical Infrastructure Issues

GAO
Accountability • Integrity • Reliability
Highlights

Highlights of GAO-03-1154T, testimony before the Senate Committee on Commerce, Science, and Transportation

September 9, 2003

TRANSPORTATION SECURITY

Federal Action Needed to Enhance Security Efforts

Why GAO Did This Study

The economic well being of the United States is dependent on the expeditious flow of people and goods through the transportation system. The attacks on September 11, 2001, illustrate the threats to and vulnerabilities of the transportation system. Prior to September 11, the Department of Transportation (DOT) had primary responsibility for the security of the transportation system. In the wake of September 11, Congress created the Transportation Security Administration (TSA) within DOT and gave it primary responsibility for the security of all modes of transportation. TSA was recently transferred to the new Department of Homeland Security (DHS). GAO was asked to examine the challenges in securing the transportation system and the federal role and actions in transportation security.

What GAO Recommends

In a June 2003 report, GAO recommended that TSA and DOT use a mechanism, such as a memorandum of agreement, to define and clarify each entity's role and responsibilities in transportation security matters. DHS and DOT disagreed with the recommendation. Based on the uncertainty in the entities' roles and responsibilities that transportation stakeholders surfaced to us, we continue to believe our recommendation is valid and would help address transportation security challenges.

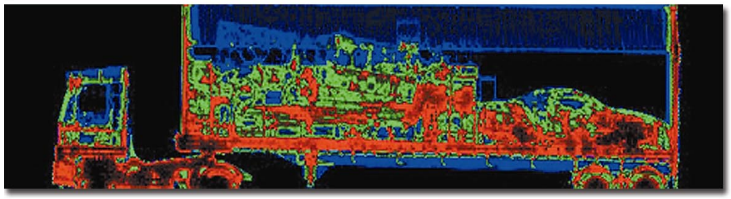
www.gao.gov/cgi-bin/getrpt?GAO-03-1154T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Peter Guerrero at (202) 512-2834 or guerrerop@gao.gov.

What GAO Found

Securing the nation's transportation system is fraught with challenges. The transportation system crisscrosses the nation and extends beyond our borders to move millions of passengers and tons of freight each day. The extensiveness of the system as well as the sheer volume of passengers and freight moved makes it both an attractive target and difficult to secure. Addressing the security concerns of the transportation system is further complicated by the number of transportation stakeholders that are involved in security decisions, including government agencies at the federal, state, and local levels and thousands of private sector companies. Further exacerbating these challenges are the financial pressures confronting transportation stakeholders. For example, the sluggish economy has weakened the transportation industry's financial condition by decreasing ridership and revenues. The federal government has provided additional funding for transportation security since September 11, but demand has far outstripped the additional amounts made available. It will take the collective effort of all transportation stakeholders to meet existing and future transportation challenges.

Since September 11, transportation stakeholders have acted to enhance security. At the federal level, TSA primarily focused on meeting aviation security deadlines during its first year of existence and DOT launched a variety of security initiatives to enhance the other modes of transportation. For example, the Federal Transit Administration provided grants for emergency drills and conducted security assessments at the largest transit agencies, among other things. TSA has recently focused more on the security of the maritime and land transportation modes and is planning to issue security standards for all modes of transportation. DOT is also continuing their security efforts. However, the roles and responsibilities of TSA and DOT in securing the transportation system have not been clearly defined, which creates the potential for overlap, duplication, and confusion as both entities move forward with their security efforts.



The Vehicle and Cargo Inspection System is a mobile nonintrusive imaging system used in the inspection of trucks, containers, and cargo and passenger vehicles. The picture on the left shows a truck moving through the inspection equipment. Inspectors use the images produced by the system (below) to determine the contents of the vehicle.

Source: Science Applications International Corporation (SAIC) ©2003.

Mr. Chairman and Members of the Committee:

We appreciate the opportunity to provide testimony on the security of our nation's transportation system. Almost 2 years have passed since the attacks of September 11, 2001, demonstrated the vulnerabilities of the nation's transportation system to the terrorist threat. Although most of the early attention following the September 11 attacks focused on aviation security, emphasis on the other modes of transportation has since grown as concerns are voiced about possible vulnerabilities, such as attempts to introduce weapons of mass destruction into this country through ports or launch chemical attacks on mass transit systems. The entire transportation industry has remained on a heightened state of alert since the attacks.

My testimony today examines (1) challenges in securing the nation's transportation system; (2) actions transportation operators,[1] as well as state and local governments, have taken since September 11 to enhance security; (3) the federal role in securing the transportation system and actions the federal government has taken to enhance transportation security since September 11; and (4) future actions that are needed to further enhance the security of the nation's transportation system. My comments are based on our recent report[2] on the security of the transportation system that we prepared for several Members of this

[1]Transportation operators may be private, public, or quasi-public entities that provide transportation services.

[2]U.S. General Accounting Office, *Transportation Security: Federal Action Needed to Help Address Security Challenges*, GAO-03-843 (Washington, D.C.: June 30, 2003). For this report, we analyzed the Federal Bureau of Investigation's threat assessment and the administration's security strategies, the Transportation Security Administration (TSA) and the Department of Transportation (DOT) security-related documents and reports, and relevant statutes and regulations. In addition, we interviewed officials from DOT, the National Railroad Passenger Corporation (Amtrak), and TSA as well as representatives from numerous transportation industry associations and transportation security experts. We selected transportation industry and state and local government associations that represent the different modes of transportation and levels of government. We selected transportation security experts on the basis of their knowledge and expertise and reputation as being experts in the transportation security arena. We also consulted with the National Academy of Sciences in identifying appropriate transportation security experts. Finally, we reviewed our past reports on homeland, port, transit, and aviation security and other research on terrorism and transportation security. We conducted our work from February 2003 through May 2003, in accordance with generally accepted government auditing standards.

Committee as well as a body of our work undertaken since September 11 on homeland security and combating terrorism.[3]

Summary

Transportation stakeholders face numerous challenges in securing the nation's transportation system. Some of these challenges are common to all modes of transportation; other challenges are specific to aviation, maritime, or land transportation modes. Common security challenges include the extensiveness of the transportation system, the interconnectivity of the system, funding limitations, and the number of stakeholders involved in transportation security. For example, the transportation system includes about 3.9 million miles of roads, over 100,000 miles of rail, almost 600,000 bridges, over 300 ports, 2.2 million miles of pipelines, 500 train stations, and over 5,000 public-use airports. The size of the system simultaneously provides a substantial number of potential targets for terrorists and makes it difficult to secure. Additionally, the number of stakeholders—including over 20 federal entities, state and local governments, and hundreds of thousands of private businesses—can lead to coordination, communication, and consensus-building challenges. Further exacerbating these challenges are the financial pressures confronting transportation stakeholders. For example, the sluggish economy has weakened the transportation industry's financial condition by decreasing ridership and revenues. The federal government has provided additional funding for transportation security since September 11, but demand has far outstripped the additional amounts made available. The aviation, maritime, and land transportation modes also face particular challenges in enhancing security. For instance, maritime and land transportation systems generally have open access designs so that users can enter the systems at multiple points; however, this openness leaves them vulnerable because transportation operators cannot monitor or control who enters or leaves the systems.

Despite these challenges, transportation operators and state and local governments have implemented numerous actions to enhance security since September 11. Although security was always a priority, the terrorist attacks elevated the importance and urgency of security. According to representatives from a number of industry associations we interviewed, transportation operators have implemented new security measures or

[3]See Related GAO Products at the end of this testimony.

increased the frequency or intensity of existing activities. For example, many transportation operators conducted risk or security assessments, undertook emergency drills, and developed security plans. State and local governments, which play a critical role in securing the system because they own a large portion of the transportation system as well as serve as first responders to incidents involving transportation assets, have also acted to improve the security of the transportation system. Some examples of their actions since September 11 include deploying additional law enforcement personnel and participating in emergency drills with the transportation industry.

The roles of federal government agencies in securing the nation's transportation system are in transition. Prior to September 11, DOT had primary responsibility for the security of the transportation system. In the wake of September 11, Congress created TSA and gave it responsibility for the security of all modes of transportation. During TSA's first year of existence, its primary focus was on aviation security. While TSA was focusing on aviation security, DOT modal administrations[4] launched various initiatives to enhance the security of the maritime and land transportation modes. For example, the Federal Transit Administration (FTA) launched a multipart security initiative to enhance transit security, which included grants for emergency drills, security assessments, and training. TSA has started to assert a greater role in securing the maritime and land transportation modes and is launching a number of new security initiatives. For example, TSA is planning to issue security standards for all modes of transportation. However, a number of representatives from transportation industry and state and local government associations that we contacted expressed concerns about not being adequately involved in TSA's decision-making, such as the development of security standards. DOT modal administrations are also continuing their transportation security efforts. For example, the Federal Highway Administration (FHWA) is coordinating a series of workshops this year on emergency response and preparedness for state departments of transportation and other agencies. The roles and responsibilities of TSA and DOT in transportation security have yet to be clearly delineated, which creates the potential for duplicating and/or conflicting efforts as both entities move forward with their security efforts.

[4]DOT's modal administrations are the departmental units responsible for the different modes of transportation, such as the Federal Railroad Administration or the Federal Highway Administration.

Transportation security experts and representatives from transportation industry and state and local government associations that we spoke with identified a number of actions that they said should be implemented to enhance the security of the nation's transportation system. In general, they believe that the transportation system is generally more secure today than it was prior to September 11; however, all noted that more work is needed to improve the security of the system. Transportation security experts and representatives from transportation industry and state and local government associations identified a number of future actions needed and stated that the identified actions are primarily the responsibility of the federal government. For instance, representatives from industry and state and local government associations told us that clarifying federal roles and coordinating federal efforts are important because association members are not clear about which agency to contact for their various security concerns and which agency has oversight for certain issues. Some representatives from the transportation industry and state and local government associations also noted that they have received conflicting messages from the different federal entities.

In our June report, we recommended that the Secretary of Homeland Security and the Secretary of Transportation develop mechanisms, such as a memorandum of agreement, to clearly define the roles and responsibilities of TSA and DOT in transportation security matters.[5] DOT and DHS generally agreed with the report's findings; however, they disagreed with the conclusions and recommendation that their roles and responsibilities in transportation security matters need to be clarified. On the basis of our discussions with transportation security stakeholders, we continue to believe our recommendation would help address transportation security challenges. For example, representatives from several associations stated that their members were unclear as to which agency to contact for their various security concerns and which agency has oversight for certain issues. Furthermore, both DOT and TSA are moving forward with their security efforts, and both entities have statutory responsibilities for transportation security. Therefore, we retained our recommendation that DOT and DHS clarify and delineate their roles and responsibilities in security matters and communicate this information to stakeholders.

[5]GAO-03-843.

Background

The nation's transportation system is a vast, interconnected network of diverse modes. Key modes of transportation include aviation; highways; motor carrier (i.e., trucking); motor coach (i.e., intercity bus); maritime; pipeline; rail (passenger and freight); and transit (e.g., buses, subways, ferry boats, and light rail). The transportation modes work in harmony to facilitate mobility through an extensive network of infrastructure and operators, as well as through the vehicles and vessels that permit passengers and freight to move within the system. For example, the nation's transportation system moves over 30 million tons of freight and provides approximately 1.1 billion passenger trips each day. The diversity and size of the transportation system make it vital to our economy and national security, including military mobilization and deployment.

Private industry, state and local governments, and the federal government all have roles and responsibilities in securing the transportation system. Private industry owns and operates a large share of the transportation system. For example, almost 2,000 pipeline companies and 571 railroad companies own and operate the pipeline and freight railroad systems, respectively. Additionally, 83 passenger air carriers and 640,000 interstate motor coach and motor carrier companies operate in the United States. State and local governments also own significant portions of the highways, transit systems, and airports in the country. For example, state and local governments own over 90 percent of the total mileage of highways. State and local governments also administer and implement regulations for different sectors of the transportation system and provide protective and emergency response services through various agencies. Although the federal government owns a limited share of the transportation system, it issues regulations, establishes policies, provides funding, and/or sets standards for the different modes of transportation. The federal government uses a variety of policy tools, including grants, loan guarantees, tax incentives, regulations, and partnerships, to motivate or mandate state and local governments or the private sector to help address security concerns.

Prior to September 11, DOT was the primary federal entity involved in transportation security matters. However, in response to the attacks on September 11, Congress passed the Aviation and Transportation Security Act (ATSA), which created TSA within DOT and defined its primary responsibility as ensuring security in all modes of transportation.[6] The act

[6]P.L. No. 107-71, 115 Stat. 597 (2001).

also gives TSA regulatory authority over all transportation modes. Since its creation in November 2001, TSA has focused primarily on meeting the aviation security deadlines contained in ATSA. With the passage of the Homeland Security Act on November 25, 2002, TSA, along with over 20 other agencies, was transferred to the new Department of Homeland Security (DHS).[7]

The Transportation System as a Whole Faces Numerous Challenges

The United States maintains the world's largest and most complex national transportation system. Improving the security of such a system is fraught with challenges for both public and private entities. To provide safe transportation for the nation, these entities must overcome issues common to all modes of transportation as well as issues specific to the individual modes of transportation.

All Modes of Transportation Face Common Challenges

Although each mode of transportation is unique, they all face some common challenges in trying to enhance security. Common challenges stem from the extensiveness of the transportation system, the interconnectivity of the system, funding security improvements, and the number of stakeholders involved in transportation security.

Size and Diversity of Transportation Modes Create Security Challenges

The size of the transportation system makes it difficult to adequately secure. The transportation system's extensive infrastructure crisscrosses the nation and extends beyond our borders to move millions of passengers and tons of freight each day. The extensiveness of the infrastructure as well as the sheer volume of freight and passengers moved through the system creates an infinite number of targets for terrorists. Furthermore, as industry representatives and transportation security experts repeatedly noted, the extensiveness of the infrastructure makes equal protection for all assets impossible.

Protecting transportation assets from attack is made more difficult because of the tremendous variety of transportation operators. Some are multibillion-dollar enterprises, and others have very limited facilities and very little traffic. Some are public agencies, such as state departments of transportation, and some are private businesses. Some transportation operators carry passengers, and others haul freight. Additionally, the type of freight moved through the different modes is similarly varied. For

[7]P.L. No. 107-296, 116 Stat. 2135 (2002).

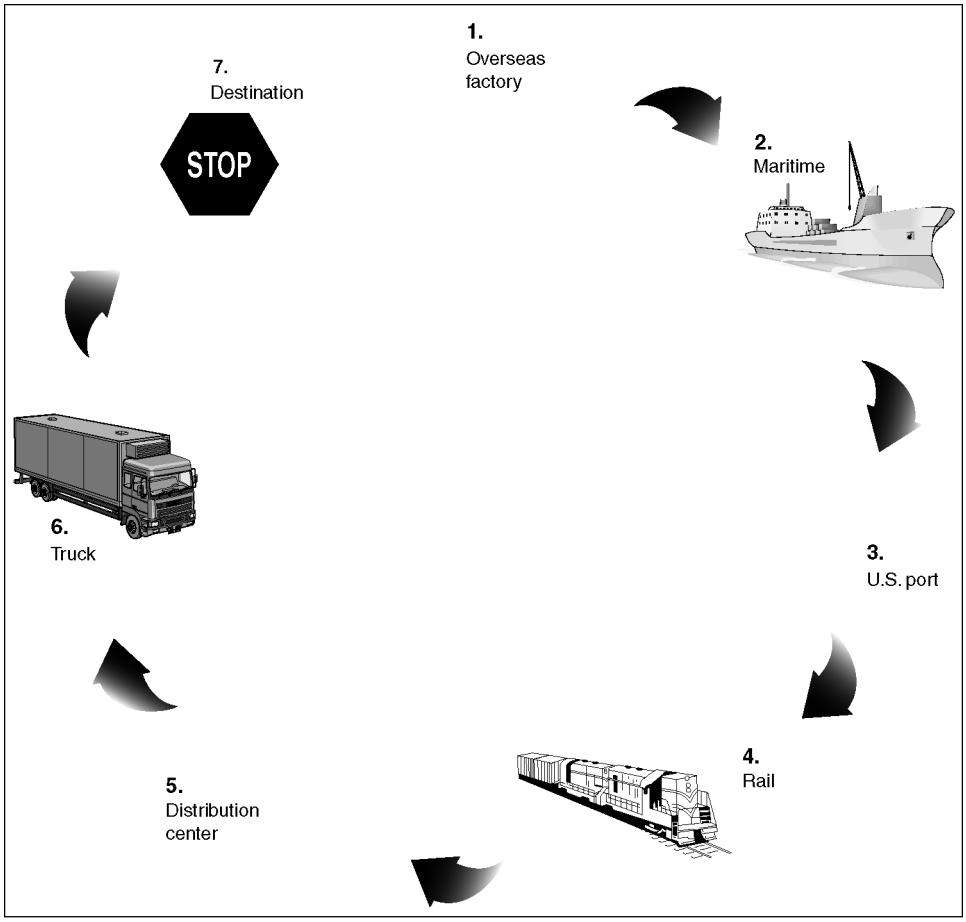
example, the maritime, motor carrier, and rail operators haul freight as diverse as dry bulk (grain) and hazardous materials.

Interconnectivity and Interdependency Also Present Challenges

Additional challenges are created by the interconnectivity and interdependency among the transportation modes and between the transportation sector and nearly every other sector of the economy. The transportation system is interconnected or intermodal because passengers and freight can use multiple modes of transportation to reach a destination. For example, from its point of origin to its destination, a piece of freight, such as a shipping container, can move from ship to train to truck. (See fig. 1.) The interconnective nature of the transportation system creates several security challenges. First, the effects of events directed at one mode of transportation can ripple throughout the entire system. For example, when the port workers in California, Oregon, and Washington went on strike in 2002, the railroads saw their intermodal traffic decline by almost 30 percent during the first week of the strike, compared with the year before. Second, the interconnecting modes can contaminate each other—that is, if a particular mode experiences a security breach, the breach could affect other modes.[8] An example of this would be if a shipping container that held a weapon of mass destruction arrived at a U.S. port where it was placed on a truck or train. In this case, although the original security breach occurred in the port, the rail or trucking industry would be affected as well. Thus, even if operators within one mode established high levels of security they could be affected because of the security efforts, or lack thereof, of the other modes. Third, intermodal facilities where a number of modes connect and interact—such as ports—are potential targets for attack because of the presence of passengers, freight, employees, and equipment at these facilities.

[8]Similarly, there are opportunities for cross contamination within the same mode. For example, a bag containing an explosive device could be placed on one airline and then transferred to another airline where it explodes.

Figure 1: Illustration of Possible Freight Movements within the Transportation System



Source: GAO.

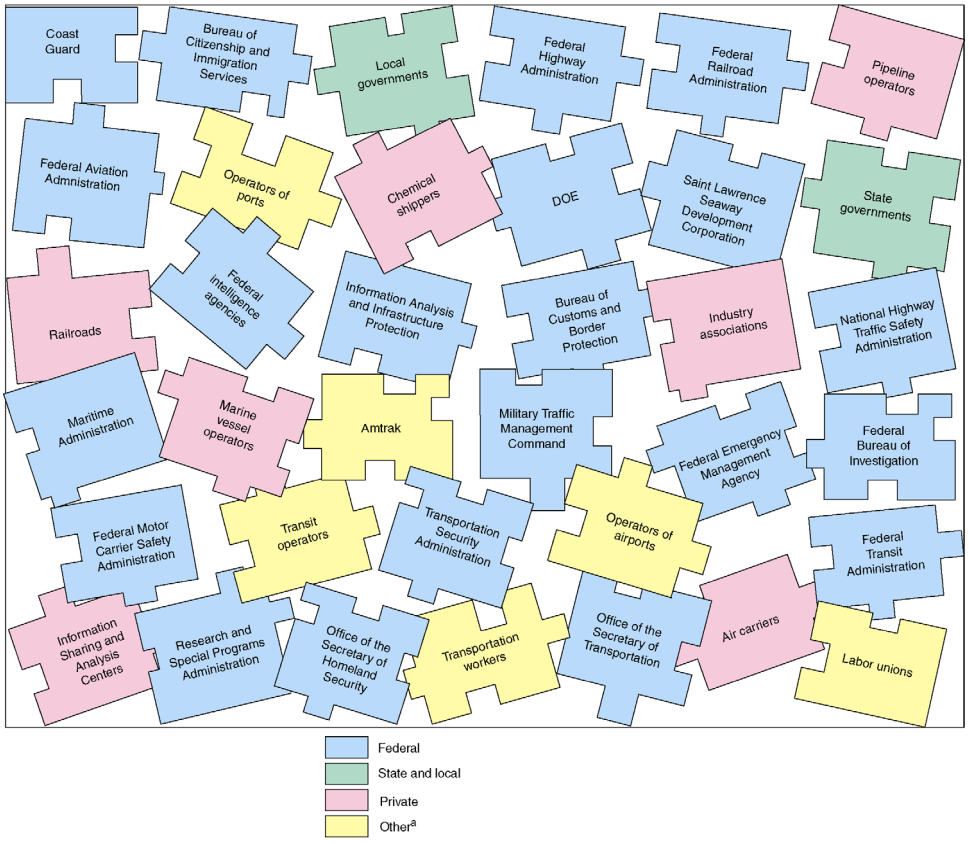
Interdependencies also exist between transportation and nearly every other sector of the economy. Consequently, an event that affects the transportation sector can have serious impacts on other industries. For example, when the war in Afghanistan began in October 2001, the rail industry restricted the movement of many hazardous materials, including chlorine, because of a heightened threat of a terrorist attack. However, within days, many major water treatment facilities reported that they were running out of chlorine, which they use to treat drinking water, and would have to shut down operations if chlorine deliveries were not immediately resumed.

The Number of Stakeholders Creates Challenges

Securing the transportation system is made more difficult because of the number of stakeholders involved. As illustrated in figure 2, numerous entities at the federal, state, and local levels, including over 20 federal entities and thousands of private sector businesses, play a key role in transportation security. For example, the Departments of Energy, Transportation, and Homeland Security; state governments; and about 2,000 pipeline operators are all responsible for securing the pipeline system. The number of stakeholders involved in transportation security can lead to communication challenges, duplication, and conflicting guidance. Representatives from several state and local government and industry associations told us that their members are receiving different messages from the various federal agencies involved in transportation security. For instance, one industry representative noted that both TSA and DOT asked the industry to implement additional security measures when the nation's threat condition was elevated to orange at the beginning of the Iraq War;[9] however, TSA and DOT were not consistent in what they wanted done—that is, they were asking for different security measures. Moreover, many representatives commented that the federal government needs to better coordinate its security efforts. These representatives noted that dealing with multiple agencies on the same issues and topics is frustrating and time consuming for the transportation sector.

[9]DHS created the Homeland Security Advisory System. The system has five threat conditions—ranging from low to severe—representing different levels of risk for terrorist attacks.

Figure 2: Key Stakeholders in Transportation Security



Source: GAO.

[a]"Other" includes private, public, or quasi-public entities.

The number of stakeholders also makes it difficult to achieve the needed cooperation and consensus to move forward with security efforts. As we have noted in past reports, coordination and consensus-building are critical to successful implementation of security efforts. Transportation stakeholders can have inconsistent goals or interests, which can make consensus-building challenging. For example, from a safety perspective, vehicles that carry hazardous materials should be required to have placards that identify the contents of a vehicle so that emergency personnel know how best to respond to an incident. However, from a security perspective, identifying placards on vehicles that carry hazardous materials make them a potential target for attack.

Funding Is Key Challenge

According to transportation security experts and state and local government and industry representatives we contacted, funding is the

most pressing challenge to securing the nation's transportation system. Although some security improvements are inexpensive, such as removing trash cans from subway platforms, most require substantial funding. Additionally, given the large number of assets to protect, the sum of even relatively less expensive investments can be cost prohibitive. For example, reinforcing shipping containers to make them more blast resistant is one way to improve security, which would cost about $15,000 per container. With several million shipping containers in use, however, this tactic would cost billions of dollars if all of them were reinforced. The total cost of enhancing the security of the entire transportation system is unknown; however, given the size of the system, it could amount to tens of billions of dollars.

The current economic environment makes this a difficult time for private industry or state and local governments to make security investments. According to industry representatives and experts we contacted, most of the transportation industry operates on a very thin profit margin, making it difficult for the industry to pay for additional security measures. The sluggish economy has further weakened the transportation industry's financial condition by decreasing ridership and revenues. For example, airlines are in the worst fiscal crisis in their history, and several have filed for bankruptcy. Similarly, the motor coach and motor carrier industries and Amtrak report decreased revenues because of the slow economy. In addition, nearly every state and local government is facing a large budget deficit for fiscal year 2004. For example, the National Governors Association estimates that states are facing a total budget shortfall of $80 billion for fiscal year 2004. Given the tight budget environment, state and local governments and transportation operators must make difficult trade-offs between transportation security investments and other needs, such as service expansion and equipment upgrades. According to the National Association of Counties, many local governments are planning to defer some maintenance of their transportation infrastructure to pay for some security enhancements.

Further exacerbating the problem of funding security improvements is the additional costs the transportation sector incurs when the federal government elevates the national threat condition. Industry representatives stated that operators tighten security, such as increasing security patrols, when the national threat condition is raised or intelligence information suggests an increased threat against their mode. However, these representatives stated that these additional measures drain resources and are not sustainable. For example, Amtrak estimates that it spends an additional $500,000 per month for police overtime when

the national threat condition is increased. Transportation industry representatives also noted that employees are diverted from their regular duties to implement additional security measures, such as guarding entranceways, in times of increased security, which hurts productivity.

The federal government has provided additional funding for transportation security since September 11, but demand has far outstripped the additional amounts made available. For example, Congress appropriated a total of $241 million for grants for ports, motor carriers, and Operation Safe Commerce in 2002.[10] However, as table 1 shows, the grant applications TSA has received for these security grants totaled $1.8 billion—nearly 8 times more than the amount available. Due to the costs of security enhancements and the transportation industries' and state and local governments' tight budget environments, the federal government is likely to be viewed as a source of funding for at least some of these enhancements. However, given the constraints on the federal budget as well as competing claims for federal assistance, requests for federal funding for transportation security enhancements will likely continue to exceed available resources.

[10]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.

Table 1: Comparison of Selected Transportation Security Grant Requests with Federal Funding Available, 2002 to 2003

(Dollars in millions)

Type of grant	Amount appropriated	Total amount requested in all grant applications
Port security grants[a]	$93.3	$697
Port security grants[b]	105	996
Intercity bus grants[b]	15	45.6
Operation Safe Commerce grants[b]	28	97.9
Total	**$241.3**	**$1,836.5**

Source: TSA.

Note: Both the Department of Defense and Emergency Supplemental Appropriations Act (P.L. No. 107-117) and the Supplemental Appropriations Act (P.L. No. 107-206) provided funding for port security grants.

[a]P.L. No. 107-117, 115 Stat. 2230 (2002).

[b]P.L. No. 107-206, 116 Stat. 820 (2002).

Balancing Potential Economic Impacts and Security Enhancements Is Also Challenging

Another challenge is balancing the potential economic impacts of security enhancements with the benefits of such measures. Although there is broad support for greater security, this task is a difficult one because the nation relies heavily on a free and expeditious flow of goods. Particularly with "just-in-time" deliveries, which require a smooth and expeditious flow through the transportation system, delays or disruptions in the supply chain could have serious economic impacts. As the Coast Guard Commandant stated about the flow of goods through ports, "even slowing the flow long enough to inspect either all or a statistically significant random selection of imports would be economically intolerable."[11]

Furthermore, security measures may have economic and competitive ramifications for individual modes of transportation. For instance, if the federal government imposed a particular security requirement on the rail industry and not on the motor carrier industry, the rail industry might incur additional costs and/or lose customers to the motor carrier industry. Striking the right balance between increasing security and protecting the

[11]*Meeting the Homeland Security Challenge: A Principled Strategy for a Balanced and Practical Response* (September 2001); and *Global Trade: America's Achilles' Heel* (February 2002) by Admiral James M. Loy and Captain Robert G. Ross, U.S. Coast Guard.

economic vitality of the national economy and individual modes will remain an important and difficult task.

Individual Transportation Modes Also Confront Unique Challenges

In addition to the overarching challenges that transportation stakeholders will face in attempting to improve transportation security, they also face a number of challenges specific to the aviation, maritime, and land transportation modes. Although aviation security has received a significant amount of attention and funding since September 11, more work is needed. In general, transportation security experts believe that the aviation system is more secure today than it was prior to September 11. However, aviation experts and TSA officials noted that significant vulnerabilities remain. For example:

- **Perimeter security**: Terrorists could launch attacks, such as launching shoulder-fired missiles, from a location just outside an airport's perimeter. Since September 11, airport operators have increased their patrols of airport perimeter areas, but industry officials state that they do not have enough resources to completely protect against these attacks.

- **Air cargo security:** 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. For example, employees of shippers and freight forwarders are not universally subject to background checks. Theft is also a major problem in air cargo shipping, signifying that unauthorized personnel may still be gaining access to air cargo shipments. Air cargo shipments pass through several hands in going from sender to recipient, making it challenging to implement a system that provides adequate security for air cargo. According to TSA officials, TSA is developing a strategic plan to address air cargo security and has undertaken a comprehensive outreach process to strengthen security programs across the industry.

- **General aviation security:** Although TSA has taken several actions related to general aviation[12] since September 11, this segment of the industry remains potentially more vulnerable than commercial aviation. For example, general aviation pilots are not screened prior to taking off, and the contents of a plane are not examined at any point. According to

[12]General aviation includes more than 200,000 corporate and privately owned aircraft at over 19,000 airports.

TSA, solutions that can be implemented relatively easily at the nation's commercial airports are not practical at the 19,000 general aviation airports. It would be very difficult to prevent a general aviation pilot intent on committing a terrorist attack with his or her aircraft from doing so. The vulnerability of the system was illustrated in January 2002, when a teenage flight student from Florida crashed his single-engine airplane into a Tampa skyscraper. TSA is working with the appropriate stakeholders to close potential security gaps and to raise the security standards across this diverse segment of the aviation industry.

Maritime and land transportation systems have their own unique security vulnerabilities. For example, maritime and land transportation systems generally have an open design, meaning the users can access the system at multiple points. The systems are open by design so that they are accessible and convenient for users. In contrast, the aviation system is housed in closed and controlled locations with few entry points. The openness of the maritime and land transportation systems can leave them vulnerable because transportation operators cannot monitor or control who enters or leaves the systems. However, adding security measures that restrict the flow of passengers or freight through the systems could have serious consequences for commerce and the public.

Individual maritime and land transportation modes also have unique challenges and vulnerabilities. For example, representatives from the motor carrier industry noted that the high turnover rate (about 40 to 60 percent) of drivers means that motor carrier operators must be continually conducting background checks on new drivers, which is expensive and time consuming. Additionally, as we noted in our report on rail safety and security,[13] the temporary storage of hazardous materials in unsecured or unmonitored rail cars while awaiting delivery to their ultimate destinations is a potential vulnerability. Specifically, unmonitored chemical cars could develop undetected leaks that could threaten the nearby population and environment. In addition, representatives from the motor coach industry commented that the number of used motor coaches on the market, coupled with the lack of guidance or requirements on buying or selling these vehicles, is a serious vulnerability. In particular, there are approximately 5,000 used motor coaches on the market; however, there is very little information on who is selling and buying them, nor is there any

[13]U.S. General Accounting Office, *Rail Safety and Security: Some Actions Already Taken to Enhance Rail Security, but Risk-based Plan Needed*, GAO-03-435 (Washington, D.C.: Apr. 30, 2003).

consistency among motor coach operators in whether they remove their logos from the vehicles before they are sold. These vehicles could be used as weapons or to transport weapons. Federal Motor Carrier Safety Administration officials told us they have not issued guidance to the industry on this potential vulnerability because TSA is responsible for security and therefore would be responsible for issuing such guidance.

Transportation Operators and State and Local Governments Have Taken Steps to Improve Security

Since September 11, transportation operators and state and local governments have been working to strengthen security, according to associations we contacted. Although security was a priority before September 11, the terrorist attacks elevated the importance and urgency of transportation security for transportation operators and state and local governments. According to representatives from a number of industry associations we interviewed, transportation operators have implemented new security measures or increased the frequency or intensity of existing activities. Some of the most common measures cited include conducting vulnerability or risk assessments, tightening access control, intensifying security presence, increasing emergency drills, developing or revising security plans, and providing additional training. (Figure 3 is a photograph from an annual emergency drill conducted by the Washington Metropolitan Area Transit Authority.)

Figure 3: Emergency Drill in Progress

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

Source: GAO.

As we have previously reported, state and local governments are critical stakeholders in the nation's homeland security efforts. This is equally true in securing the nation's transportation system. State and local governments play a critical role, in part, because they own a significant portion of the transportation infrastructure, such as airports, transit systems, highways, and ports. For example, state and local governments own over 90 percent of the total mileage of the highway system. Even when state and local governments are not the owners or operators, they nonetheless are directly affected by the transportation modes that run through their jurisdictions. Consequently, the responsibility for protecting this infrastructure and responding to emergencies involving the transportation infrastructure often falls on state and local governments.

Security efforts of local and state governments have included developing counter terrorist plans, participating in training and security-related research, participating in transportation operators' emergency drills and table-top exercises, conducting vulnerability assessments of transportation assets, and participating in emergency planning sessions with transportation operators. Some state and local governments have also hired additional law enforcement personnel to patrol transportation assets. Much of the funding for these efforts has been covered by the state and local governments, with a bulk of the expenses going to personnel costs, such as for additional law enforcement officers and overtime.

Congress and Federal Agencies Have Taken Numerous Actions to Enhance Security, but Roles Remain Unclear

Congress, DOT, TSA, and other federal agencies have taken numerous steps to enhance transportation security since September 11. The roles of the federal agencies in securing the nation's transportation system, however, are in transition. Prior to September 11, DOT had primary responsibility for the security of the transportation system. In the wake of September 11, Congress created TSA and gave it responsibility for the security of all modes of transportation. However, DOT and TSA have not yet formally defined their roles and responsibilities in securing all modes of transportation. Furthermore, TSA is moving forward with plans to enhance transportation security. For example, TSA plans to issue security standards for all modes. DOT modal administrations are also continuing their security efforts for different modes of transportation.

Congress and Federal Agencies Have Acted to Enhance Transportation Security

Congress has acted to enhance the security of the nation's transportation system since September 11. In addition to passing the Aviation and Transportation Security Act (ATSA),[14] Congress passed a number of other key pieces of legislation aimed at improving transportation security. For example, Congress passed the USA PATRIOT Act of 2001,[15] which mandates federal background checks of individuals operating vehicles carrying hazardous materials; and the Homeland Security Act,[16] which created DHS and moved TSA to the new department.[17] Congress also provided funding for transportation security enhancements through various appropriations acts. For example, the 2002 Supplemental Appropriations Act, in part, provided (1) $738 million for the installation of explosives detection systems in commercial service airports, (2) $125 million for port security activities, and (3) $15 million to enhance the security of intercity bus operations.

[14]P.L. No. 107-71, 115 Stat. 597 (2001).

[15]P.L. No. 107-56, 115 Stat. 272 (2001).

[16]P.L. No. 107-296, 116 Stat. 2135 (2002).

[17]The U.S. Coast Guard was also transferred to DHS. In the *Terms of Reference Regarding the Respective Roles of the U.S. Coast Guard and the Transportation Security Administration*, the Coast Guard is designated as the lead DHS agency for maritime security and is directed to coordinate as appropriate with other agencies. The document further notes that a supporting memorandum of agreement between the Commandant of the Coast Guard and the Administrator of the Transportation Security Administration is being developed.

Federal agencies, notably TSA and DOT, have also taken steps to enhance transportation security since September 11. In its first year of existence, TSA worked to establish its organization and focused primarily on meeting the aviation security deadlines contained in ATSA. In January 2002, TSA had 13 employees to tackle securing the nation's transportation system; 1 year later, TSA had about 65,000 employees. TSA reports that it met over 30 deadlines during 2002 to improve aviation security, including two of its most significant deadlines—to deploy federal passenger screeners at airports across the nation by November 19, 2002; and to screen every piece of checked baggage for explosives by December 31, 2002.[18] According to TSA, other completed TSA activities included recruiting, hiring, training, and deploying about 56,000 federal screeners; awarding grants for port security; and implementing performance management system and strategic planning activities to create a results-oriented culture.

As TSA worked to establish itself and improve the security of the aviation system, DOT modal administrations acted to enhance the security of air, land, and maritime transportation. (See app. I for a table listing the actions taken by DOT modal administrations since September 11.) The actions taken by the DOT modal administrations have varied. For example, FTA launched a multipart initiative for mass transit agencies that provided grants for emergency drills, offered free security training, conducted security assessments at 36 transit agencies, provided technical assistance, and invested in research and development. The Federal Motor Carrier Safety Administration developed three courses for motor coach drivers. The responses of the various DOT modal agencies have varied due to differences in authority and resource limitations.

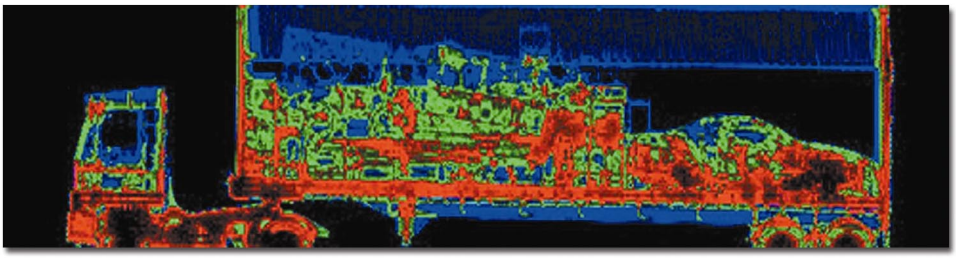
In addition to TSA and DOT modal administrations, other federal agencies have also taken actions to improve security. For example, the Bureau of Customs and Border Protection (CBP), previously known as the U.S. Customs Service, has launched a number of initiatives aimed at

[18]The Homeland Security Act, P.L. 107-296 (November 25, 2002) the legislation that created DHS, amended this deadline to allow some airports up to an extra year (December 31, 2003) to deploy all of the necessary explosive detection equipment to enable TSA to screen all checked baggage. TSA reported that as of December 31, 2002, about 90 percent of all checked baggage were screened with an explosive detection system or explosives trace detection equipment and the remaining checked baggage was screened using alternative means as is allowed under the law.

strengthening the security of the U.S. border.[19] Some of the specific security initiatives that CBP has implemented include establishing the Customs Trade Partnership Against Terrorism (C-TPAT), which is a joint government business initiative aimed at securing the supply chain of global trade against terrorist exploitation; and launching the Container Security Initiative (CSI), which is designed specifically to secure ocean-going sea containers. In addition, CBP has developed and/or deployed tools to detect weapons of mass destruction in cargo containers and vehicles, such as the new mobile gamma ray imaging devices pictured in figure 4.

Figure 4: Photograph of Inspection Equipment in Use

The Vehicle and Cargo Inspection System is a mobile nonintrusive imaging system used in the inspection of trucks, containers, and cargo and passenger vehicles. The picture on the left shows a truck moving through the inspection equipment. Inspectors use the images produced by the system (below) to determine the contents of the vehicle.



Source: Science Applications International Corporation (SAIC) ©2003.

TSA Moves Forward as its Role in Transportation Security Evolves

TSA is moving forward with efforts to secure the entire transportation system. TSA has adopted a systems approach—that is, a holistic rather than a modal approach—to securing the transportation system. In addition, TSA is using risk management principles to guide its decision-

[19]The U.S. Customs Service was transferred from the Department of Treasury to DHS in the Homeland Security Act of 2002 (P.L. No. 107-296, 116 Stat. 2135 (2002)) and renamed the Bureau of Customs and Border Protection.

making. TSA is also planning to establish security standards for all modes of transportation and is launching a number of new security efforts for the maritime and land transportation modes.

TSA Adopts a Systems Approach and Risk Management Principles

Using the systems approach, TSA plans to address the security of the entire transportation system as a whole, rather than focusing on individual modes of transportation. According to TSA officials, using a systems approach to security is appropriate for several reasons. First, the transportation system is intermodal, interdependent, and international. Given the intermodalism of the system, incidents in one mode of transportation could affect other modes. Second, it is important not to drive terrorism from one mode of transportation to another mode because of perceived lesser security—that is, make a mode of transportation a more attractive target because another mode is "hardened" with additional security measures. Third, it is important that security measures for one mode of transportation are not overly stringent or too economically challenging compared with the measures used for other modes. Fourth, it is important that the attention on one aspect of transportation security (e.g., cargo, infrastructure, or passengers) does not leave the other aspects vulnerable.

TSA has also adopted a risk management approach for its efforts to enhance the security of the nation's transportation system. 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 in order to link resources with prioritized efforts. (See app. II for a description of the key elements of a risk management approach.) The highest priorities emerge where the three elements of risk management overlap. For example, transportation infrastructure that is determined to be a critical asset, vulnerable to attack, and a likely target would be most at risk and therefore would be a higher priority for funding compared with infrastructure that was only vulnerable to attack. According to TSA officials, risk management principles will drive all decisions—from standard-setting to funding priorities to staffing.

Using risk management principles to guide decision-making is a good strategy, given the difficult trade-offs TSA will likely have to make as it moves forward with its security efforts. We have advocated using a risk management approach to guide federal programs and responses to better prepare against terrorism and other threats and to better direct finite national resources to areas of highest priority. As representatives from local government and industry associations and transportation security experts repeatedly noted, the size of the transportation system precludes

equal protection for all assets; moreover, the risks vary by transportation assets within modes and by modes. In addition, requests for funding for transportation security enhancements will likely exceed available resources. Risk management principles can help TSA determine security priorities and identify appropriate solutions.

TSA Plans to Issue National Security Standards

TSA plans to issue national security standards for all modes of transportation. The federal government has historically set security standards for the aviation sector. For instance, prior to the passage of ATSA, FAA set security standards that the airlines were required to follow in several areas including, screening equipment, screener qualifications, and access control systems. In contrast, prior to the September 11 attacks, limited statutory authority existed to require measures to ensure the security of the maritime and land transportation systems. According to a TSA report, the existing regulatory framework leaves the maritime and land transportation systems unacceptably vulnerable to terrorist attack. For example, the rail, transit, and motor coach transportation systems are subject to no mandatory security requirements, resulting in little or no screening of passengers, baggage, or crew. Additionally, seaborne passenger vessel and seaport terminal operators have inconsistent levels and methods of screening and are largely free to set their own rules about the hiring and training of security personnel. Hence, TSA will set standards to ensure consistency among modes and across the transportation system and to reduce the transportation system's vulnerability to attacks.[20]

According to TSA officials and documents, TSA's standards will be performance-, risk-, and threat-based and may be mandatory. More specifically:

- **Standards will be performance-based.** Rather than being prescriptive standards, TSA standards will be performance-based, which will allow

[20]The Information Analysis and Infrastructure Protection Directorate within DHS is working with TSA, the Coast Guard, and other federal agencies on developing a set of national standards that would apply to all ports. These efforts are well under way. The Coast Guard has been developing a set of standards since May 2002 as part of its efforts to conduct vulnerability assessments for all U.S. ports. The standards will go into effect on July 1, 2004, as part of the International Convention for the Safety of Life at Sea (SOLAS) amendments and the International Ship and Port Facility Security Code (ISPS) that was adopted by the International Maritime Organization conference in December 2002. The Coast Guard considers that the implementation of these standards is best done through mandating compliance with the SOLAS amendments and the ISPS Code. According to TSA, because of the Coast Guard's significant role in securing maritime transportation, TSA will likely play a coordination role in the maritime arena.

transportation operators to determine how best to achieve the desired level of security. TSA officials believe that performance-based standards provide for operator flexibility, allow operators to use their professional judgment in enhancing security, and encourage technology advancement.

- **Standards will be risk-based.** Standards will be set for areas for which assessments of the threats, vulnerabilities, and criticality indicate that an attack would have a national impact. A number of factors could be considered in determining "national impact," such as fatalities and economic damage.

- **Standards will be threat-based.** The standards will be tied to the national threat condition and/or local threats. As the threat condition escalates, the standards will require transportation operators to implement additional countermeasures.

- **Standards may be mandatory.** The standards will be mandatory when the risk level is too high or unacceptable. TSA officials stated that in these cases, mandatory standards are needed to ensure accountability. In addition, according to TSA officials, voluntary requirements put security-conscious transportation operators that implement security measures at a competitive disadvantage—that is, they have spent money that their competitors may not have spent. This creates a disincentive for transportation operators to implement voluntary requirements. TSA officials believe that mandatory standards will reduce this problem. In determining whether mandatory standards are needed, TSA will review the results of criticality and vulnerability assessments, current best practices, and voluntary compliance opportunities in conjunction with the private sector and other government agencies.

  Although TSA officials expect some level of resistance to the standards by the transportation industry, they believe that their approach of using risk-, threat-, and performance-based standards will increase the acceptance of the standards. For example, performance-based standards allow for more operator flexibility in implementing the standards, compared with rigid, prescriptive standards. Moreover, TSA plans to issue only a limited number of standards—that is, standards will be issued only when assessments of the threats, vulnerabilities, and criticality indicate that the level of risk is too high or unacceptable.

  TSA also expects some level of resistance to the standards from DOT modal administrations. Although TSA will establish the security standards, TSA expects that they will be administered and implemented by existing agencies and organizations. DOT modal administrations may be reluctant

to assume this role because doing so could alter their relationships with the industry. Historically, the missions of DOT surface transportation modal administrations have largely focused on maintaining operations and improving service and safety, not regulating security. Moreover, the authority to regulate security varies by DOT modal administration. For example, FTA has limited authority to regulate and oversee security at transit agencies. In contrast, FRA has regulatory authority for rail security, and DOT's Office of Pipeline Safety has responsibility for writing safety and security regulations for liquefied natural gas storage facilities. In addition, DOT modal administrations may be reluctant to administer and implement standards because of resource concerns. FHWA officials commented that given the current uncertainty about the standards and their impacts, FHWA is reluctant to commit, in advance, staff or funding to enforce new security standards.

Gaining Stakeholder Buy-in is Critical for Standards to Work, but Stakeholders Express Concerns

Because transportation stakeholders will be involved in administering, implementing, and/or enforcing TSA standards, stakeholder buy-in is critical to the success of this initiative. Compromise and consensus on the part of stakeholders are also necessary. However, achieving such consensus and compromise may be difficult, given the conflicts between some stakeholders' goals and interests.

Transportation stakeholders we contacted also expressed a number of concerns about TSA's plan to issue security standards for all modes of transportation. For example, industry associations expressed concerns that the standards would come in the form of unfunded mandates—that is, the federal government would not provide funding to implement mandatory standards. According to the industry and state and local government associations we spoke to, unfunded mandates create additional financial burdens for transportation operators, who are already experiencing financial difficulties. Industry representatives also expressed concern that TSA has not adequately included the transportation industry in its development of standards. Many industry representatives and some DOT officials we met with were unsure of whether TSA was issuing standards, what the standards would entail, or the time frames for issuing the standards. The uncertainty about the pending standards can lead to confusion and/or inaction. For example, Amtrak officials noted that they are reluctant to spend money to implement certain security measures because they are worried that TSA will subsequently issue standards that will require Amtrak to redo its efforts. Transportation stakeholders also raised other concerns about TSA's plans to issues standards, including questioning whether TSA has the necessary expertise to develop

appropriate standards and whether mandatory standards, as opposed to voluntary standards, are prudent.

TSA Is Launching Other Security Initiatives

TSA is also working on a number of additional security efforts, such as establishing the Transportation Workers Identification Card (TWIC) program; developing the next generation of the Computer Assisted Passenger Pre-Screening System; developing a national transportation system security plan; and exploring methods to integrate operations and security, among other things. The TWIC program is intended to improve access control for the 12 million transportation workers who require unescorted physical or cyber access to secure areas of the nation's transportation modes by establishing a uniform, nationwide standard for secure identification of transportation workers. Specifically, TWIC will combine standard background checks and biometrics so that a worker can be positively matched to his/her credential. Once the program is fully operational, the TWIC would be the standard credential for transportation workers and would be accepted by all modes of transportation. According to TSA, developing a uniform, nationwide standard for identification will minimize redundant credentialing and background checks.

DOT Modal Agencies Are Continuing Forward with Their Security Efforts

As TSA moves forward with new security initiatives, DOT modal administrations are also continuing their security efforts and, in some cases, launching new security initiatives. For example, FHWA is coordinating a series of workshops this year on emergency response and preparedness for state departments of transportation and other agencies. FTA also has a number of initiatives currently under way in the areas of public awareness, research, training, technical assistance, and intelligence sharing. For example, FTA developed a list of the top 20 security actions transit agencies should implement and is currently working with transit agencies to assist them in implementing these measures.

FAA is also continuing its efforts to enhance cyber security in the aviation system. Although the primary responsibility for securing the aviation system was transferred to TSA, FAA remains responsible for protecting the nation's air traffic control system—both the physical security of its air traffic control facilities and computer systems. The air traffic control system's computers help the nation's air traffic controllers to safely direct and separate traffic—sabotaging this system could have disastrous consequences. FAA is moving forward with efforts to increase the physical security of its air traffic control facilities and ensure that contractors who have access to the air traffic control system undergo background checks.

TSA's and DOT's Roles and Responsibilities Have Not Been Clearly Defined

The roles and responsibilities of TSA and DOT in transportation security have yet to be clearly delineated, which creates the potential for duplicating or conflicting efforts as both entities move forward with their security efforts. DOT modal administrations were primarily responsible for the security of the transportation system prior to September 11. In November 2001, Congress passed ATSA, which created TSA and gave it primary responsibility for securing all modes of transportation.[21] However, during TSA's first year of existence, TSA's main focus was on aviation security—more specifically, on meeting ATSA deadlines. While TSA was primarily focusing on aviation security, DOT modal administrations launched various initiatives to enhance the security of the maritime and land transportation modes. With the immediate crisis of meeting many aviation security deadlines behind it, TSA has been able to focus more on the security of all modes of transportation.

Legislation has not specifically defined TSA's role and responsibilities in securing all modes of transportation. In particular, ATSA does not specify TSA's role and responsibilities in securing the maritime and land transportation modes in detail as it does for aviation security. For instance, the act does not set deadlines for TSA to implement certain transit security requirements. Instead, the act simply states that TSA is responsible for ensuring security in all modes of transportation. The act also did not eliminate the existing statutory responsibilities for DOT modal administrations to secure the different transportation modes. Moreover, recent legislation indicates that DOT still has security responsibilities. In particular, the Homeland Security Act of 2002 states that the Secretary of Transportation is responsible for the security as well as the safety of rail and the transport of hazardous materials by all modes.

To clarify their roles and responsibilities in transportation security, DOT modal administrations and TSA planned to develop memorandums of agreement. The purpose of these documents was to define the roles and responsibilities of the different agencies for transportation security and address a variety of issues, including separating safety and security activities, interfacing with the transportation industry, and establishing funding priorities. TSA and the DOT modal administrations worked for months to develop the memorandums of agreement and the draft agreements were presented to senior DOT and TSA management for review in early spring of this year. According to DOT's General Counsel,

[21]P.L. No. 107-71, 115 Stat. 597 (2001).

with the exception of the memorandum of agreement between FAA and TSA, the draft memorandums were very general and did not provide much clarification. Consequently, DOT and TSA decided not to sign the memorandums of agreement, except for the memorandum of agreement between FAA and TSA, which was signed on February 28, 2003.[22]

The General Counsel suggested several reasons why the majority of the draft memorandums of agreement were too general. First, as TSA's departure date approached—that is, the date that TSA transferred from DOT to DHS—TSA and DOT modal administration officials may have grown concerned about formally binding the organizations to specific roles and responsibilities. Second, the working relationships between TSA and most of the DOT modal administrations are still very new; as a result, all of the potential issues, problem areas, or overlap have yet to be identified. Thus, identifying items to include in the memorandums of agreement was more difficult.

Rather than execute memorandums of agreement, the Secretary of Transportation and the Administrator of TSA exchanged correspondence that commits each entity to continued coordination and collaboration on security measures. In the correspondence, the Secretary and Administrator also agreed to use the memorandum of agreement between TSA and FAA as a framework for their interactions on security matters for all other modes. TSA and DOT officials stated that they believe memorandums of agreement are a good strategy for delineating roles and responsibilities and said that they would be open to using memorandums of agreement in the future.

[22]DOT and TSA have signed other memorandums of agreement that are narrow in scope and address a specific issue. For example, TSA and DOT signed a memorandum of agreement regarding the processing of civil rights complaints.

Experts and Associations Identified Future Actions to Advance the Security of the Transportation System

Transportation security experts and representatives of state and local government and industry associations we contacted generally believe that the transportation system is more secure today than it was prior to September 11. Transportation stakeholders have worked hard to strengthen the security of the system. Nevertheless, transportation experts, industry representatives, and federal officials all recommend that more work be done. Transportation experts and state and local government and industry representatives identified a number of actions that, in their view, the federal government should take to enhance security, including clarifying federal roles and coordinating federal efforts, developing a transportation security strategy, funding security enhancements, investing in research and development, and providing better intelligence information and related guidance. Specifically:

- Clarify federal roles and responsibilities. The lack of clarity about the roles and responsibilities of federal entities in transportation security creates the potential for confusion, duplication, and conflicts. Understanding roles, responsibilities, and whom to call is crucial in an emergency. However, representatives from several industry associations stated that their members were unclear about which agency to contact for their various security concerns and which agency has oversight for certain issues. Furthermore, they said that they do not have contacts within these agencies. As mentioned earlier, several industry representatives reported that their members are receiving different messages from various federal agencies involved in transportation security, which creates confusion and frustration within the industry. According to industry representatives and transportation security experts, uncertainty about federal roles and the lack of coordination are straining intergovernmental relationships, draining resources, and raising the potential for problems in responding to terrorism. One industry association told us, for instance, that it has been asked by three different federal agencies to participate in three separate studies of the same issue.

- **Establish a national transportation strategy.** A national strategy is crucial for helping stakeholders identify priorities, leveraging resources, establishing stakeholder performance expectations, and creating incentives for stakeholders to improve security. Currently, local government associations view the absence of performance expectations—coupled with limited threat information—as a major obstacle in focusing their people and resources on high-priority threats, particularly at elevated threat levels. The experts also noted that modal strategies—no matter how

complete—cannot address the complete transportation security problem and will leave gaps in preparedness. As mentioned earlier, TSA is in the process of developing a national transportation system security plan,[23] which, according to the Deputy Administrator of TSA, will provide an overarching framework for the security of all modes.

- **Provide funding for needed security improvements.** Although an overall security strategy is a prerequisite to investing wisely, providing adequate funding also is essential, according to experts we contacted. Setting security goals and strategies without adequate funding diminishes stakeholders' commitment and willingness to absorb initial security investments and long-term operating costs, an expert emphasized. Industry and state and local government associations also commented that federal funding should accompany any federal security standards; otherwise, mandatory standards will be considered unfunded mandates that the industry and state and local governments will have to absorb.

- **Invest in research and development for transportation security.** According to most transportation security experts and associations we contacted, investing in research and development is an appropriate role for the federal government, because the products of research and development endeavors would likely benefit the entire transportation system, not just individual modes or operators. TSA is actively engaged in research and development projects, such as the development of the next generation explosive detection systems for baggage, hardening of aircraft and cargo/baggage containers, biometrics and other access control methods, and human factors initiatives to identify methods to improve screener performance, at its Transportation Security Laboratory in Atlantic City, New Jersey. However, TSA noted that continued adequate funding for research and development is paramount in order for TSA to be able to meet security demands with up-to-date and reliable technology.

- Provide timely intelligence information and related guidance. Representatives from numerous associations commented that the federal government needs to provide timely, localized, actionable intelligence information. They said that general threat warnings are not helpful. Rather, transportation operators want more specific intelligence information so that they can understand the true nature of a potential threat and implement appropriate security measures. Without more localized and actionable intelligence, stakeholders said they run the risk of

[23]TSA hopes to have a draft of the national transportation system security plan prepared by the end of this year.

wasting resources on unneeded security measures or not providing an adequate level of security. Moreover, local government officials often are not allowed to receive specific intelligence information because they do not have appropriate federal security clearances. Also, there is little federal guidance on how local authorities should respond to a specific threat or general threat warnings. For example, San Francisco police were stationed at the Golden Gate Bridge to respond to the elevated national threat condition. However, without information about the nature of the threat to San Francisco's large transportation infrastructure or clear federal expectations for a response, it is difficult to judge whether actions like this are the most effective use of police protection, according to representatives from a local government association.

Observations

Securing the transportation system is fraught with challenges. Despite these challenges, transportation stakeholders have worked to strengthen security since September 11. However, more work is needed. It will take the collective effort of all transportation stakeholders to meet the continuing challenges and enhance the security of the transportation system.[24]

During TSA's first year of existence, it met a number of challenges, including successfully meeting many congressional deadlines for aviation security. With the immediate crisis of meeting these deadlines behind it, TSA can now examine the security of the entire transportation system. As TSA becomes more active in securing the maritime and land transportation modes, it will become even more important that the roles of TSA and DOT modal administrations are clearly defined. Lack of clearly defined roles among the federal entities could lead to duplication and confusion. More importantly, it could hamper the transportation sector's ability to prepare for and respond to attacks. Therefore, in our report, we recommended that the Secretary of Homeland Security and the Secretary of Transportation develop mechanisms, such as a memorandum of agreement, to clearly define the roles and responsibilities of TSA and DOT in transportation security and communicate this information to stakeholders.

[24]See appendix III for a listing of active GAO engagements related to transportation security.

This concludes my prepared statement. I would be pleased to respond to any questions you or other Members of the Committee may have.

For information about this testimony, please contact Peter Guerrero, Director, Physical Infrastructure Issues, on (202) 512-2834. Individuals making key contributions to this testimony included Cathleen Berrick, Steven Calvo, Nikki Clowers, Michelle Dresben, Susan Fleming, Libby Halperin, David Hooper, Hiroshi Ishikawa, and Ray Sendejas.

Appendix I: Key Transportation Security Efforts of DOT Modal Administrations, September 2001 to May 2003

Mode	DOT modal administration	Examples of actions taken
All (transport of hazardous materials)	Research and Special Programs Administration (Office of Hazardous Materials Safety)	• Established regulations for shippers and transporters of certain hazardous materials to develop and implement security plans and to require security awareness training for hazmat employees. • Developed hazardous materials transportation security awareness training for law enforcement, the industry, and the hazmat community. • Published security advisory, which identifies measures that could enhance the security of the transport of hazardous materials. • Investigated the security risks associated with placarding hazardous materials, including whether removing placards from certain shipments improve shipment security, and whether alternative methods for communicating safety hazards could be deployed.
Aviation	Federal Aviation Administration	• Established rule for strengthening cockpit doors on commercial aircraft. • Issued guidance to flight school operators for additional security measures. • Assisted Department of Justice in increasing background check requirements for foreign nationals seeking pilot certificates. • Increased access restrictions at air traffic control facilities. • Developed computer security strategy.
Highways	Federal Highway Administration	• Provided vulnerability assessment and emergency preparedness workshops. • Developed and prioritized list of highway security research and development projects. • Convened blue ribbon panel on bridge and tunnel vulnerabilities.

Mode	DOT modal administration	Examples of actions taken
Maritime	U.S. Coast Guard[a] Maritime Administration	• Activated and deployed port security units to help support local port security patrols in high threat areas. • Boarded and inspected ships to search for threats and confirmed the identity of those aboard. • Conducted initial assessments of the nation's ports to identify vessel types and facilities that pose a high risk of being involved in a transportation security incident. • Established a new centralized National Vessel Movement Center to track the movement of all foreign-flagged vessels entering U.S. ports of call. • Established new guidelines for developing security plans and implementing security measures for passenger vessels and passenger terminals. • Used the pollution and hazardous materials expertise of the Coast Guard's National Strike Force to prepare for and respond to bioterrorism and weapons of mass destruction. • Increased port security and terrorism emphasis at National Port Readiness Network Port Readiness Exercises. • Provided port security training and developed standards and curriculum to educate and train maritime security personnel. • Increased access restrictions and established new security procedures for the Ready Reserve Force. Provided merchant mariner background checks for Ready Reserve Force and sealift vessels in support of Department of Defense and Coast Guard requirements. • Provided merchant mariner force protection training.
Motor carrier	Federal Motor Carrier Safety Administration	• Conducted 31,000 on-site security sensitivity visits for hazardous materials carriers; made recommendations after visits. • Initiated a field operational test to evaluate different safety and security technologies and procedures, and identify the most cost- effective means for protecting different types of hazardous cargo for security purposes. • Provided free training on trucks and terrorism to law enforcement officials and industry representatives. • Conducted threat assessment of the hazardous materials industry.
Motor coach	Federal Motor Carrier Safety Administration	• Developed three courses for drivers on security-related information, including different threats, how to deal with packages, and how to respond in the case of an emergency.

Mode	DOT modal administration	Examples of actions taken
Pipeline	Research and Special Programs Administration (Office of Pipeline Safety)	• Developed contact list of operators who own critical systems. • Convened blue ribbon panel with operators, state regulators, and unions to develop a better understanding of the pipeline system and coordinate efforts of the stakeholders. • Worked with TSA to develop inspection protocols to use for pipeline operator security inspections. The Office of Pipeline Safety and TSA have begun the inspection of major operators. • Created e:mail network of pipeline operators and a call-in telephone number that pipeline operators can use to obtain information. • Directed pipeline operators to identify critical facilities and develop security plans for critical facilities that address deterrence, preparedness, and rapid response and recovery from attacks. • Worked with industry to develop risk-based security guidance, which is tied to national threat levels and includes voluntary, recommended countermeasures.
Rail	Federal Railroad Administration	• Shared threat information with railroads and rail labor. • Reviewed Association of American Railroads' and Amtrak's security plans. • Assisted commuter railroads with their security plans. • Provided funding for security assessments of three commuter railroads, which were included in FTA's assessment efforts. • Reached out to international community for lessons learned in rail security.
Transit	Federal Transit Administration	• Awarded $3.4 million in grants to over 80 transit agencies for emergency response drills. • Offered free security training to transit agencies. • Conducted security assessments at the 36 largest transit agencies. • Provided technical assistance to 19, with a goal of 60, transit agencies on security and emergency plans and emergency response drills. • Increased funding for security research and development efforts.

Source: GAO presentation of information provided by DOT modal administrations.

[a]The U.S. Coast Guard was transferred to DHS in the Homeland Security Act of 2002 (P.L. No. 107-296, 116 Stat. 2135 (2002)).

Appendix II: Elements of a Risk Management Approach

A risk management approach encompasses three key elements—a threat assessment, vulnerability assessment, and criticality assessment. In particular, these three elements provide the following information:

- A threat assessment identifies and evaluates potential threats on the basis of such factors 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 critical 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. Thus, it helps managers determine operational requirements and target resources to the highest priorities while reducing the potential for targeting resources to lower priorities.

Appendix III: GAO Active Engagements Related to Transportation Security

TSA Baggage Screening	Key Questions: 1) What are the status and associated costs of TSA efforts to acquire, install, and operate explosive detection equipment (Electronic Trace Detection Technology and Explosive Detection Systems) to screen all checked baggage by December 31, 2003? 2) What are the benefit and tradeoffs—to include costs, operations and performance—of using alternative explosive detection technologies currently available for baggage screening?
General Aviation Security	Key Questions: 1) How has security concerns and measures at changed at general aviation airports since September 11, 2001? 2) What steps has the Transportation Security Administration taken to improve general aviation security?
Banner Pilot Waivers	Key Questions: What are procedures for conducting background and security checks for pilots of small banner-towing aircraft requesting waivers to perform stadium overflights? (2) To what extent were these procedures followed in conducting required background and security checks since 9/11? (3) How effective were these procedures in reducing risks to public safety?
U.S. Coast Guard Budget And Mission Performance	Key Questions: (1) What are the levels of effort for USCG's various missions? (2) What is USCG's progress in developing a strategic plan for setting goals for all of its various missions? (3) What is USCG's mission performance as compared to its performance and strategic plans?
Transportation Security Administration's Computer Assisted Passenger Prescreening System II (CAPPS-II)	Key Questions: 1) How will the CAPPS-II system function and what data will be needed to make the system operationally effective? 2) What safeguards will be put in place to protect the traveling public's privacy? 3) What systems and measures are in place to determine whether CAPPS-II will result in improved national security? 4) What impact will CAPPS-II have on the traveling public and airline industry in terms of costs, delays, risks, and hassle, etc.?

Transportation Security Administration Passengers Screening Program	Key Questions: 1) What efforts have been taken or planned to ensure passenger screeners comply with federal standards and other criteria, to include efforts to train, equip, and supervise passenger screeners? 2) What methods does TSA use to test screener performance, and what have been the results of these tests? 3) How have the results of tests of TSA passenger screeners compared to the results achieved by screeners prior to 9/11 and at the 5 pilot program airports? 4) What actions are TSA taking to remedy performance concerns?
TSA's Use of Sole Source Contracts	Key Questions: (1) To what extent does TSA follow applicable acquisition laws and policies, including ensuring adequate competition? (2) How well does TSA's organizational structure facilitate effective, efficient procurement? (3) How does TSA ensure that its acquisition workforce is equipped to award and oversee contracts? (4) How well do TSA's policies and processes ensure that it receives the supplies and services it needs on time and at reasonable cost?
TSA's Efforts To Implement Section 106, 136, And 138 Of The Aviation And Transportation Security Act	Key Questions: (1) What is the status of TSA's efforts to implement section 106 of the Act requiring improved airport perimeter access security? (2) What is the status of TSA's efforts to implement section 136 requiring assessment and deployment of commercially available security practices and technologies? (3) What is the status of TSA's efforts to implement section 138 requiring background investigations for TSA and other airport employees?
Implementation of the Maritime Transportation Security Act of 2002	Key Questions: 1) How effectively is the port vulnerability assessment process being implemented, and what actions are being taken to address deficiencies identified? 2) What progress is being made to develop port, vessel, and facility security plans? 3) Does the CG have sufficient resources and an action plan to ensure the plans be completed, reviewed and approved in time to meet statutory deadlines? 4) What will it cost stakeholders to comply?

Assessment of the Portable Air Defense Missile Threat	Key Questions: 1) What is the nature and extent of the threat from MANPADs? 2) How effective are U.S. controls on the use of exported MANPADs? 3) How do multilateral efforts attempt to stem MANPAD proliferation? 4) What types of countermeasures are available to minimize this threat and at what cost?
Federal Aviation Administration Designee Program	Key Questions: (1) What is the nature, scope, and operational framework of the designee program? (2) What are the identified strengths and weaknesses of the program? (3) What is the potential for FAA's ODA proposal and other stakeholders' alternatives to address the identified program weaknesses?
Custom Cargo Inspections at Seaports	Key Questions: (1) How has Customs developed the Automated Targeting System (ATS) and the new anti-terrorism rules? (2) How does Customs use ATS to identify containerized cargo as "high risk" for screening and inspection to detect cargo that might contain weapons of mass destruction (WMD)? (3) To what extent is ATS implemented at seaports, including impact and challenges involved? (4) What is Customs' plan for assessing system implementation and performance?
Enhancement Options for Intermodal Freight Transportation	Key Questions: 1) What are the current and emerging national challenges to freight mobility and what proposals have been put forth to address these issues? 2) To what extent do these current and emerging challenges exist at container ports and surrounding areas and to what extent do the proposals appear to have applicability to these locations?
Social Security Administration's Role in Verifying Identities For State's Licensing of Drivers	Key Questions: (1) What are states' policies and practices for verifying the identity of driver's license/ID card applicants and how might they more effectively use SSNs or other tools to verify identity? (2) How does SSA assist states in verifying SSNs for driver's license/ID card applicants and how can SSA improve the verification service it provides?

United States Coast Guard's National Distress and Response "Rescue 21" System Modernization	Key Questions: (1) What are the status, plans, and technical and programmatic risks associated with the National Distress and Response System (NDRS) Modernization Project? (2) How is the Coast Guard addressing concerns with the new NDRS, such as communication coverage gaps and the inability to pinpoint distressed boaters? (3) How will Coast Guard's new homeland security role affect the NDRS project?
U.S. Border Radiation Detection	Key Questions: (1) What is the status of Customs' plan to install radiation detection equipment at U.S. border crossings? (2) What is the basis for the plan's time frame? (3) What is Customs' technical capability to implement the plan? (4) How well is Customs coordinating with other agencies in the area of radiation detection? (5) What are the results of Customs' evaluations of radiation detection equipment and how are the evaluations being used?
Airline Assistance Determination Of Whether The $5 Billion Provided by P.L. 107-42 Was Used To Compensate The Nation's Major Air Carriers For Their Losses Stemming From The Events of Sept. 11, 2001	Key Questions: (1) Was the $5 billion used only to compensate major air carriers for their uninsured losses incurred as a result of the terrorist attacks? (2) Were carriers reimbursed, per the act, only for increases in insurance premiums resulting from the attacks?

Effectiveness of the Transportation Security Administration's Research and Development Program

Key Questions: (1) What is the budget profile for the Federal Aviation Administration's and the Transportation Security Administration's (TSA's) aviation security research and development (R&D) program? (2) How effective is TSA's strategy for determining which aviation security technologies to research and develop? (3) To what extent do stakeholders believe that TSA is researching and developing the most promising aviation security technologies?

Federal Air Marshals

Key Questions: (1) How has the FAM program evolved, in terms of recruiting, training, retention, and operations since the transfer of program management to TSA? (2) To what extent has TSA implemented the necessary internal controls to meet the human capital and operational challenges of the FAM program? (3) To what extent has TSA developed plans and initiatives to accommodate future FAM program sustainability, growth and maturation?

Related GAO Products

Transportation Security Reports and Testimonies

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

Transportation Security Research: Coordination Needed in Selecting and Implementing Infrastructure Vulnerability Assessments, GAO-03-502 (Washington, D.C.: May 1, 2003).

Rail Safety and Security: Some Actions Already Taken to Enhance Rail Security, but Risk-based Plan Needed, GAO-03-435 (Washington, D.C.: April 30, 2003).

Coast Guard: Challenges during the Transition to the Department of Homeland Security, GAO-03-594T (Washington, D.C.: April 1, 2003).

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

Aviation Security: Measures Needed to Improve Security of Pilot Certification Process, GAO-03-248NI (Washington, D.C.: February 3, 2003). (Not for Public Dissemination)

Major Management Challenges and Program Risks: Department of Transportation, GAO-03-108 (Washington, D.C.: January 1, 2003).

High Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructure, GAO-03-121 (Washington, D.C.: January 1, 2003).

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-03-344 (Washington, D.C.: December 20, 2002).

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

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

Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk, GAO-03-303T (Washington, D.C.: November 19, 2002).

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

Coast Guard: Strategy Needed for Setting and Monitoring Levels of Effort for All Missions, GAO-03-155 (Washington, D.C.: November 12, 2002).

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

Pipeline Safety and Security: Improved Workforce Planning and Communication Needed, GAO-02-785 (Washington, D.C.: August 26, 2002).

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

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

Critical infrastructure Protection: Significant Challenges Need to Be Addressed, GAO-02-961T (Washington, D.C.: July 24, 2002).

Combating Terrorism: Preliminary Observations on Weaknesses in Force Protection for DOD Deployments Through Domestic Seaports, GAO-02-955TNI (Washington, D.C.: July 23, 2002). (Not for Public Dissemination)

Information Concerning the Arming of Commercial Pilots, GA0-02-822R (Washington, D.C.: June 28, 2002).

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

Coast Guard: Budget and Management Challenges for 2003 and Beyond, GAO-02-538T (Washington, D.C.: March 19, 2002).

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 Illustrate Severe Weaknesses in Aviation Security, GAO-01-1166T (Washington, D.C.: September 20, 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).

Terrorism and Risk Management

Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues, GAO-03-715T (Washington, D.C.: May 8, 2003).

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

Homeland Security: Management Challenges Facing Federal Leadership, GAO-03-260 (Washington, D.C.: December 20, 2002).

Homeland Security: Information Technology Funding and Associated Management Issues, GAO-03-250 (Washington, D.C.: December 13, 2002).

Homeland Security: Information Sharing Activities Face Continued Management Challenges, GAO-02-1122T (Washington, D.C.: October 1, 2002).

National Preparedness: Technology and Information Sharing Challenges, GAO-02-1048R (Washington, D.C.: August 30, 2002).

Homeland Security: Effective Intergovernmental Coordination Is Key to Success, GAO-02-1013T (Washington, D.C.: August 23, 2002).

Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems, GAO-02-474 (Washington, D.C.: July 15, 2002).

Critical Infrastructure Protection: Significant Homeland Security Challenges Need to Be Addressed, GAO-02-918T (Washington, D.C.: July 9, 2002).

Homeland Security: Intergovernmental Coordination and Partnership Will Be Critical to Success, GAO-02-901T (Washington, D.C.: July 3, 2002).

Homeland Security: New Department Could Improve Coordination but May Complicate Priority Setting, GAO-02-893T (Washington, D.C.: June 28, 2002).

National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy, GAO-02-811T (Washington, D.C.: June 7, 2002).

Homeland Security: Responsibility and Accountability for Achieving National Goals, GAO-02-627T (Washington, D.C.: April 11, 2002).

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).

Combating Terrorism: Intergovernmental Cooperation in the Development of a National Strategy to Enhance State and Local Preparedness, GAO-02-550T (Washington, D.C.: April 2, 2002).

Combating Terrorism: Enhancing Partnerships Through a National Preparedness Strategy, GAO-02-549T (Washington, D.C.: March 28, 2002).

Combating Terrorism: Critical Components of a National Strategy to Enhance State and Local Preparedness, GAO-02-548T (Washington, D.C.: March 25, 2002).

Combating Terrorism: Intergovernmental Partnership in a National Strategy to Enhance State and Local Preparedness, GAO-02-547T (Washington, D.C.: March 22, 2002).

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

Combating Terrorism: Key Aspects of a National Strategy to Enhance State and Local Preparedness, GAO-02-473T (Washington, D.C.: March 1, 2002).

Homeland Security: Challenges and Strategies in Addressing Short- and Long-Term National Needs, GAO-02-160T (Washington, D.C.: November 7, 2001).

Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts, GAO-02-208T (Washington, D.C.: October 31, 2001).

Combating Terrorism: Considerations for Investing Resources in Chemical and Biological Preparedness, GAO-02-162T (Washington, D.C.: October 17, 2001).

Information Sharing: Practices That Can Benefit Critical Infrastructure Protection, GAO-02-24 (Washington, D.C.: October 15, 2001).

Homeland Security: Key Elements of a Risk Management Approach, GAO-02-150T (Washington, D.C.: October 12, 2001).

Chemical and Biological Defense: Improved Risk Assessment and Inventory Management Are Needed, GAO-01-667 (Washington, D.C.: September 28, 2001).

Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks, GAO-01-1168T (Washington, D.C.: September 26, 2001).

Homeland Security: A Framework for Addressing the Nation's Efforts, GAO-01-1158T (Washington, D.C.: September 21, 2001).

Combating Terrorism: Selected Challenges and Related Recommendations, GAO-01-822 (Washington, D.C.: September 20, 2001).

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Public Affairs

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