United States General Accounting Office

GAO

Report to Congressional Requesters

June 2003

TRANSPORTATION SECURITY

Federal Action Needed to Help Address Security Challenges

GAO

Accountability ★ Integrity ★ Reliability

G A O
Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-843, a report to Congressional Requesters

Why GAO Did This Study

The economic well being of the U.S. is dependent on the expeditious flow of people and goods through the transportation system. The attacks on September 11, 2001, illustrate the threats 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

GAO recommends that DHS and DOT use a mechanism, such as a memorandum of agreement, to clarify and delineate DOT's and TSA's roles and responsibilities in transportation security matters. DHS and DOT generally agreed with the report's findings; however, they 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-03-843.

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.

June 2003

TRANSPORTATION SECURITY

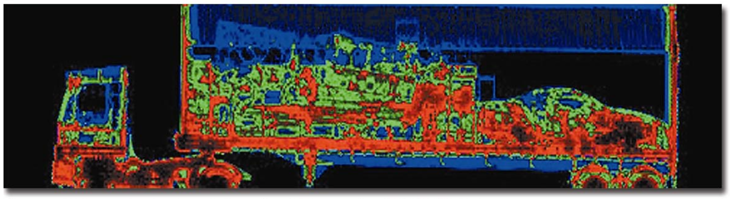
Federal Action Needed to Help Address Security Challenges

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 a 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 starting this summer. 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.

Contents

Letter

Appendixes

Related GAO Products

Tables

Figures

Abbreviations

ATSA	Aviation and Transportation Security Act
AASHTO	American Association of State Highway and Transportation Officials
CBP	Bureau of Customs and Border Protection
CSI	Container Security Initiative
C-TPAT	Customs Trade Partnership Against Terrorism
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FHWA	Federal Highway Administration
FTA	Federal Transit Administration
Amtrak	National Railroad Passenger Corporation
TSA	Transportation Security Administration
TWIC	Transportation Workers Identification Card

GAO
Accountability ★ Integrity ★ Reliability

United States General Accounting Office
Washington, D.C. 20548

June 30, 2003

Congressional Requesters

The attacks of September 11, 2001, demonstrated the vulnerabilities of the nation's transportation system to the terrorist threat. Terrorist events around the world have also shown that transportation systems are often targets of attack—roughly one-third of terrorist attacks worldwide target transportation systems.[1] While most of the early attention following the September 11 attacks focused on airport security, emphasis on the other modes of transportation has since grown as concerns are voiced about possible vulnerabilities, such as introducing weapons of mass destruction into this country through ports or launching chemical attacks on mass transit systems. The entire transportation industry has remained on a heightened state of alert since the attacks. For example, as of May 2003, the Department of Transportation (DOT) had issued over 15 terrorist threat advisories to different segments of the transportation industry since September 11.

As requested, this report examines (1) challenges in securing the nation's transportation system; (2) actions transportation operators,[2] 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. To address these objectives, we analyzed the Federal Bureau of Investigation's recent threat assessment and the administration's security strategies.[3] We also analyzed the Transportation Security Administration (TSA) and DOT security-related documents and reports as well as relevant statutes and regulations. In addition, we interviewed officials from DOT, the National Railroad Passenger Corporation (Amtrak), and TSA as well as

[1] Congressional Research Service, *Transportation Issues in the 107th Congress*, (Washington, D.C.: July 16, 2002).

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

[3] The White House, *National Strategy for The Physical Protection of Critical Infrastructures and Key Assets*, February 2003; Federal Bureau of Investigation, *The Terrorist Threat to the U.S. Homeland: An FBI Assessment*, January 2003; and The White House, *National Strategy for Homeland Security*, July 2002.

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 based on their knowledge/expertise and reputation as being an expert 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. (See app. I for a more detailed discussion of our report's scope and methodology.)

Results in Brief

Transportation stakeholders face numerous challenges in securing the nation's transportation system. Some of these challenges are common to all modes of transportation while 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 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, TSA's 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 recently 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, starting this summer. 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

[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.

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.

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 is important because their 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.

We are recommending 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. We provided draft copies of this report to Amtrak, DOT, and DHS for their review and comment. Amtrak generally agreed with our findings and recommendation and provided some technical comments, which we incorporated where appropriate. 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. We continue to believe our recommendation would help address transportation security challenges, based on our discussions with transportation security stakeholders. 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 entities are moving forward with their security efforts, and both entities have statutory responsibilities for transportation security. Therefore, we continue to recommend that DOT and DHS clarify and delineate their roles and responsibilities in security matters and communicate this information to stakeholders. (See app. II and app. III for DOT and DHS comments and our responses.)

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.

Given the important role the transportation system plays in our economy, security, and every-day life, the transportation system is considered a critical infrastructure. The USA PATRIOT Act defines critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economy security, national public health or safety, or combination of those matters."[5] In the *National Strategy for Homeland Security*, the administration identifies the transportation system as one of the 13 critical infrastructure sectors that must be protected. The administration's *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* defines the administration's plan for protecting our critical infrastructures and key assets, including the transportation system, from terrorist attacks. This strategy also outlines the guiding principles that will underpin the nation's efforts to secure the infrastructures vital to national security, governance, the economy and public confidence. The strategy is designed to serve as a foundation for building and fostering the necessary cooperation between

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

government, private industry and citizens in protecting critical infrastructures.

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 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]

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

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

Throughout the world, all modes of transportation have been targets of terrorist attacks. For example, aviation has long been an attractive target for terrorists. Aircraft hijackings became a regular occurrence in the 1970s, leading to the first efforts in aviation security. In 1988, a Pan Am flight was bombed over Lockerbie, Scotland, killing all 259 on board. In 1995, a plot to bomb as many as 11 U.S. airliners was discovered. Most recently, U.S. aircraft were hijacked on September 11, 2001, and crashed into the World Trade Center in New York City, the Pentagon in Washington, D.C., and a field in Pennsylvania, killing about 3,000 people and destroying billions of dollars' worth of property.

Public surface transportation systems have also been a common target for terrorist attacks around the world. For example, the first large-scale terrorist use of a chemical weapon occurred in 1995 on the Tokyo subway system. In this attack, a terrorist group released sarin gas on a subway train, killing 11 people and injuring 5,500. According to the Mineta Transportation Institute,[8] surface transportation systems were the target of more than 195 terrorist attacks from 1997 through 2000.

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.

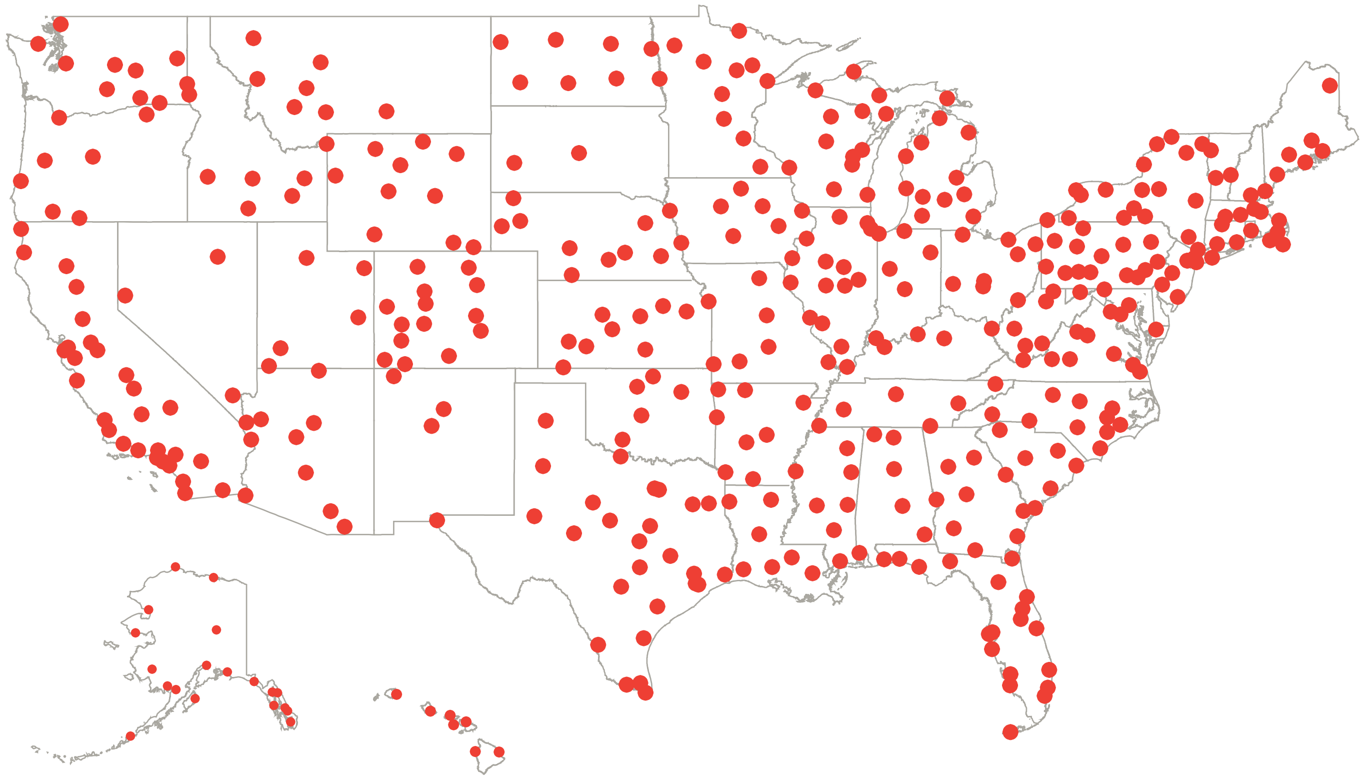
[8] Congress, as part of the Intermodal Surface Transportation Efficiency Act of 1991 (ISTEA), established the Mineta Transportation Institute. The Institute focuses on international surface transportation policy issues as related to three primary responsibilities: research, education, and technology transfer.

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. (See fig. 1 for maps of the different transportation modes.) 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 it impossible to equally protect all assets.

Figure 1: Illustration of the Extensiveness of the Different Modes of Transportation

Airports



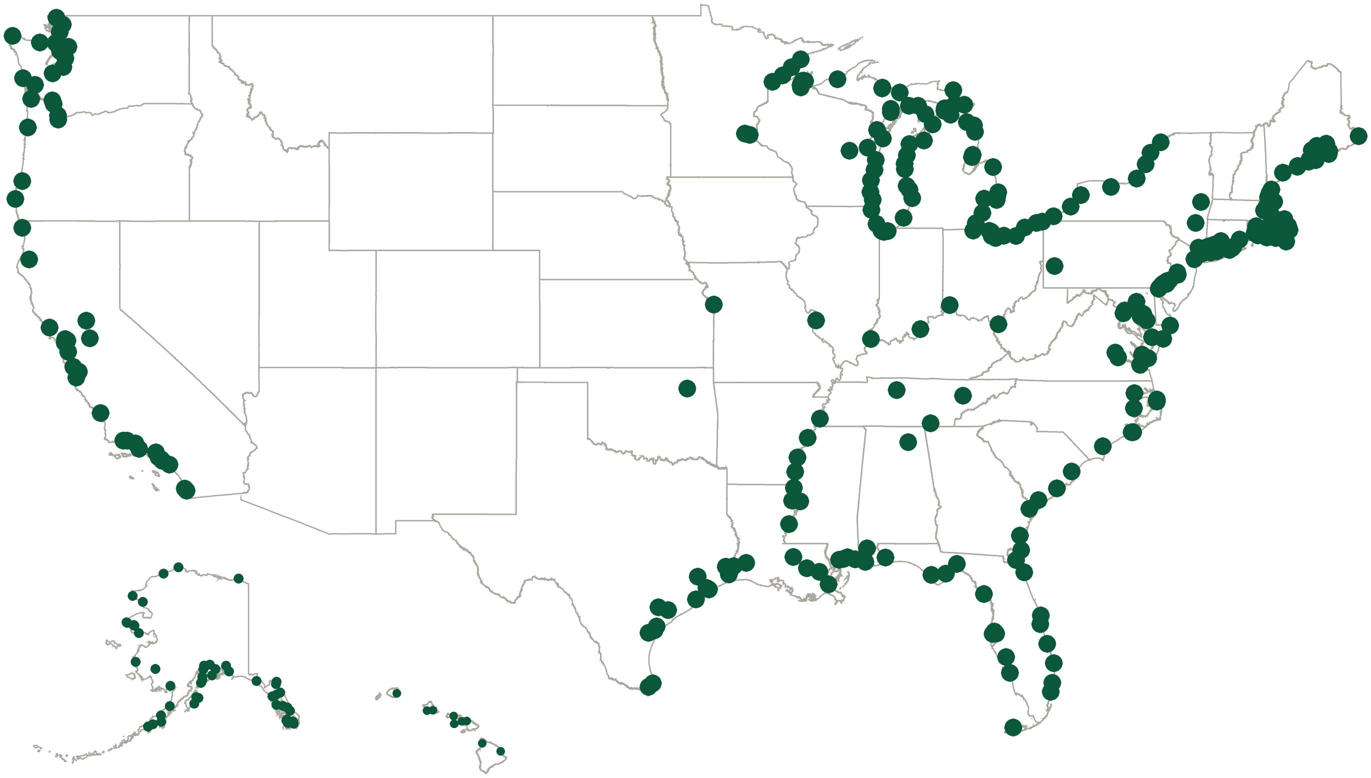
Source: GAO presentation of Bureau of Transportation statistics, TSA, and FTA data.

Note: This map shows the location of all airports with Federal Security Directors except for the nine airports in Puerto Rico, the Virgin Islands, the American Samoa, and the Mariana Islands. Federal

Security Directors are TSA employees who oversee federal security operations at the nation's airports. A total of 433 airports are shown in this map.

Illustration of the Extensiveness of the Different Modes of Transportation (Continued)

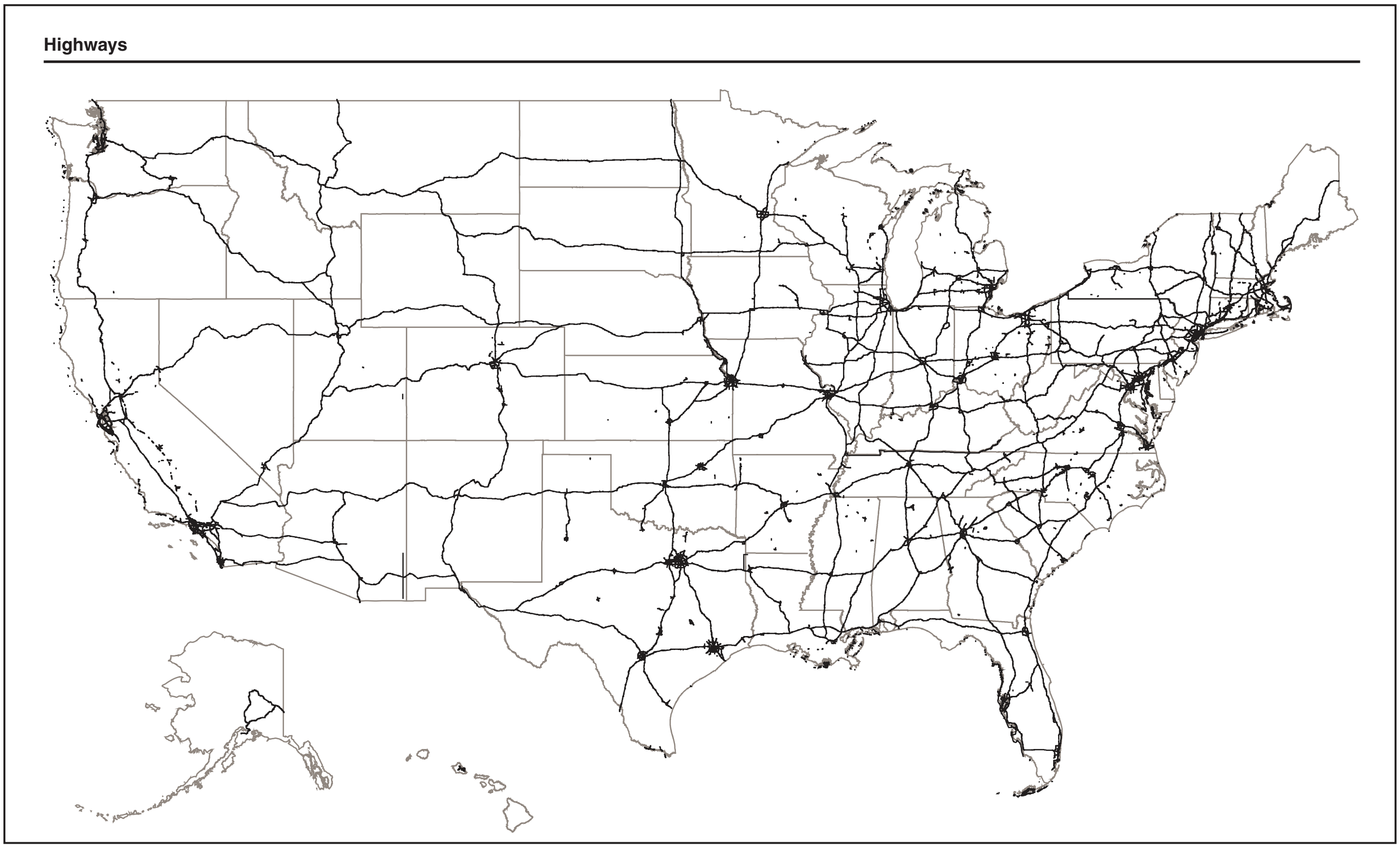
Ports



Source: GAO presentation of Bureau of Transportation statistics, TSA, and FTA data.

Note: This map shows the location of all U.S. ports for eight ports located in Puerto Rico and the Virgin Islands. A total of 353 ports are shown.

Illustration of the Extensiveness of the Different Modes of Transportation (Continued)

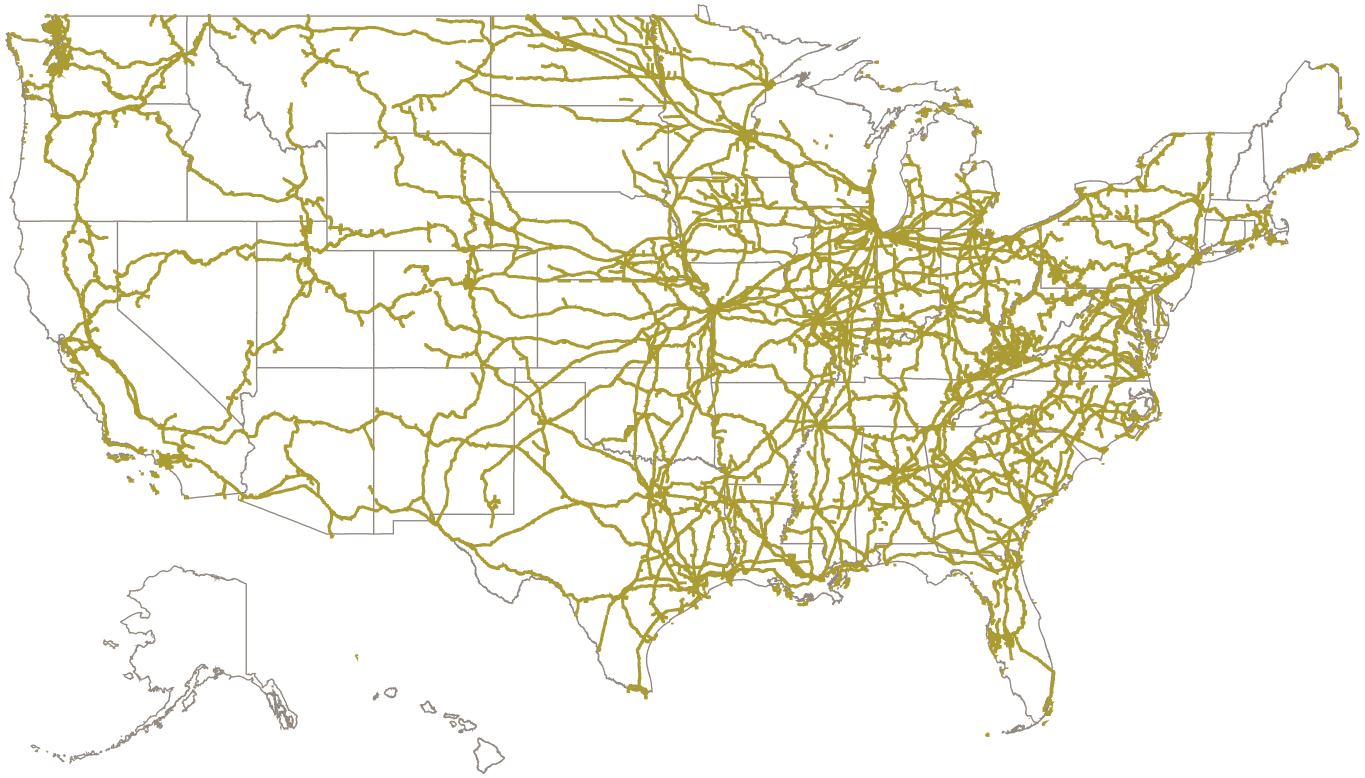


Source: GAO presentation of Bureau of Transportation statistics, TSA, and FTA data.

Note: This map shows the National Highway Planning Network. It does not show all urban and rural roads in the United States.

Illustration of the Extensiveness of the Different Modes of Transportation (Continued)

Rail

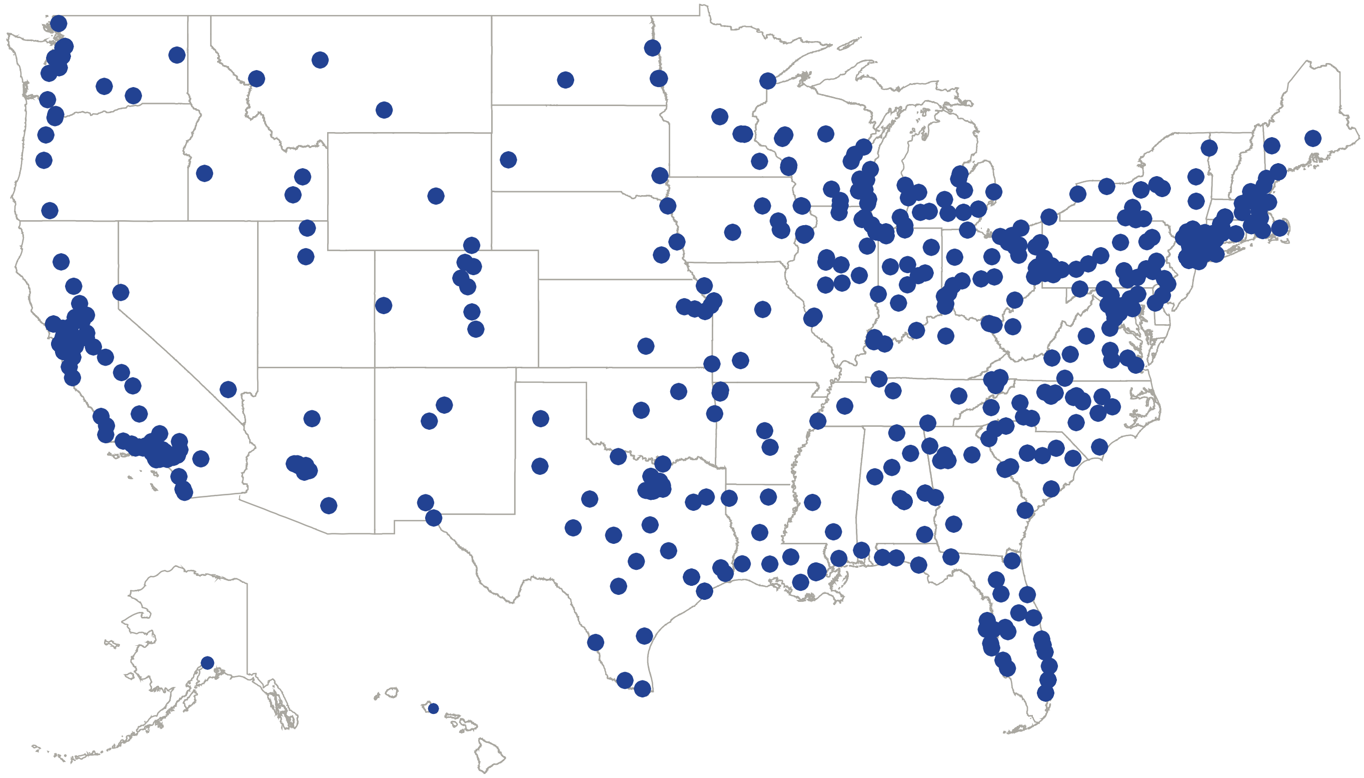


Source: GAO presentation of Bureau of Transportation statistics, TSA, and FTA data.

Note: This map shows the rail lines of Class I railroads, which are the largest railroads, as defined by operating revenue. Class I railroads represent the majority of rail freight activity.

Illustration of the Extensiveness of the Different Modes of Transportation (Continued)

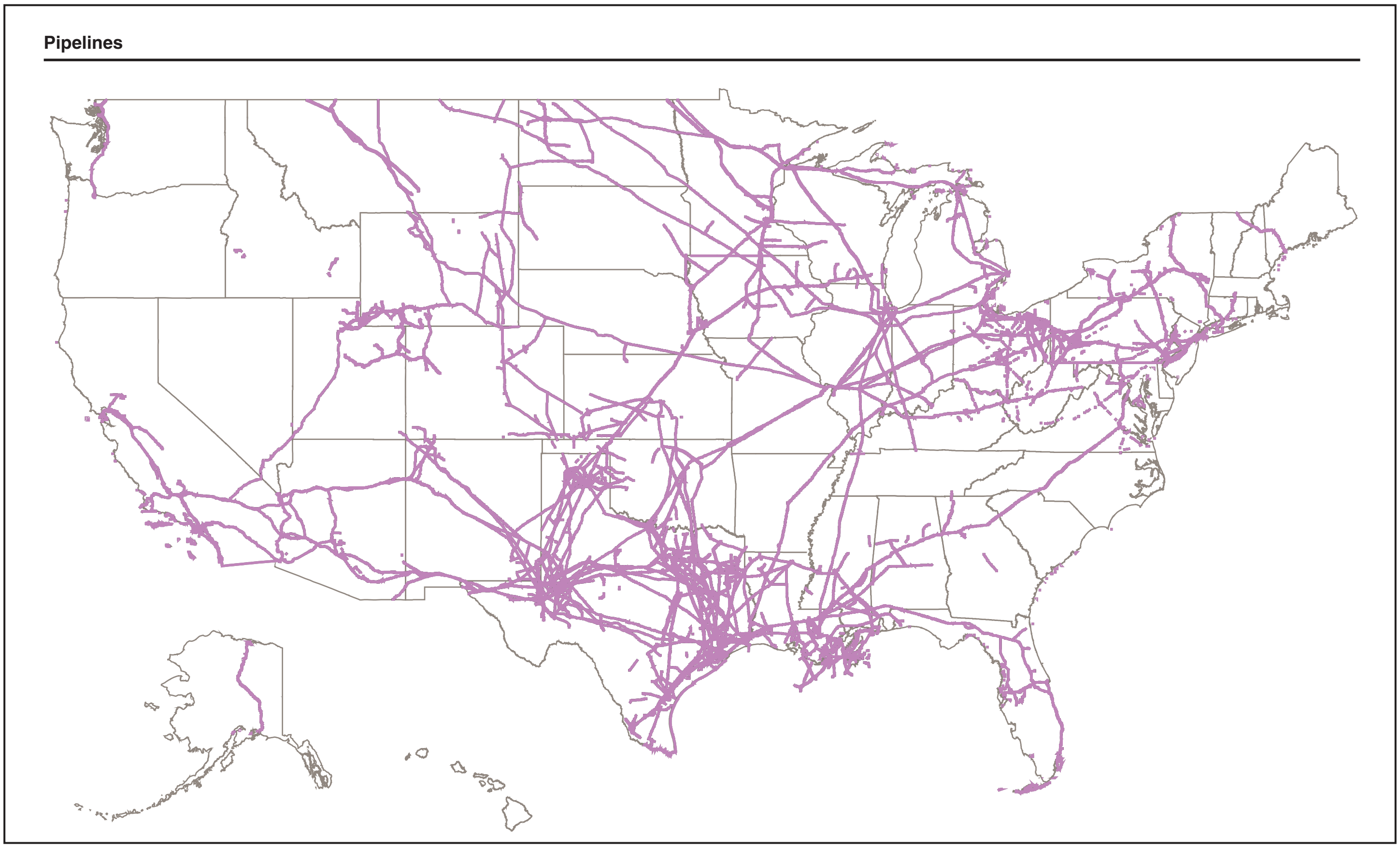
Transit



Source: GAO presentation of Bureau of Transportation statistics, TSA, and FTA data.

Note: This map shows the location of all mass transit agencies that were eligible to receive federal urbanized area formula funding in 2001, except for 13 transit agencies located in Puerto Rico. A total of 589 transit agencies are shown.

Illustration of the Extensiveness of the Different Modes of Transportation (Continued)



Source: GAO presentation of Bureau of Transportation statistics, TSA, and FTA data.

Note: This map shows the location of pipelines that are at least 12 inches in diameter, which accounts for the majority of all pipeline capacity.

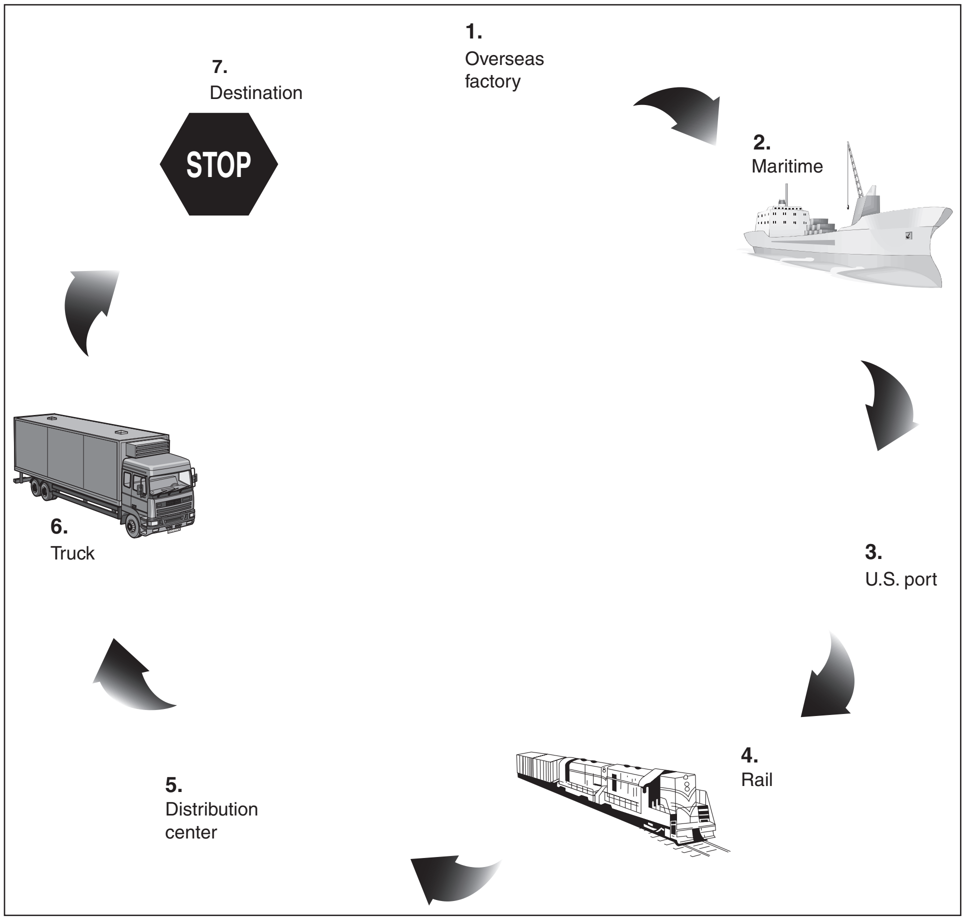
Protecting transportation assets from attack is made more difficult because of the tremendous variety of transportation operators. Some are multibillion-dollar enterprises, while others have very limited facilities and very little traffic. Some are public agencies, such as state departments of transportation, while some are private businesses. The type of freight moved through the different modes is similarly varied. For example, the maritime, motor carrier, and rail operators haul freight as diverse as dry bulk (grain) and hazardous materials. Additionally, some transportation operators carry passengers while others haul freight.

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. 2.) The interconnective nature of the transportation system creates several security challenges. First, events directed at one mode of transportation can have ripple effects 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.[9] 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 passenger, freight, employees, and equipment at these facilities. (See fig. 3.)

[9] 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 2: Illustration of Possible Freight Movements within the Transportation System



Source: GAO.

Figure 3: Intermodal Activity at a U.S. Port

Source: © 1995 Nova Development Corporation.

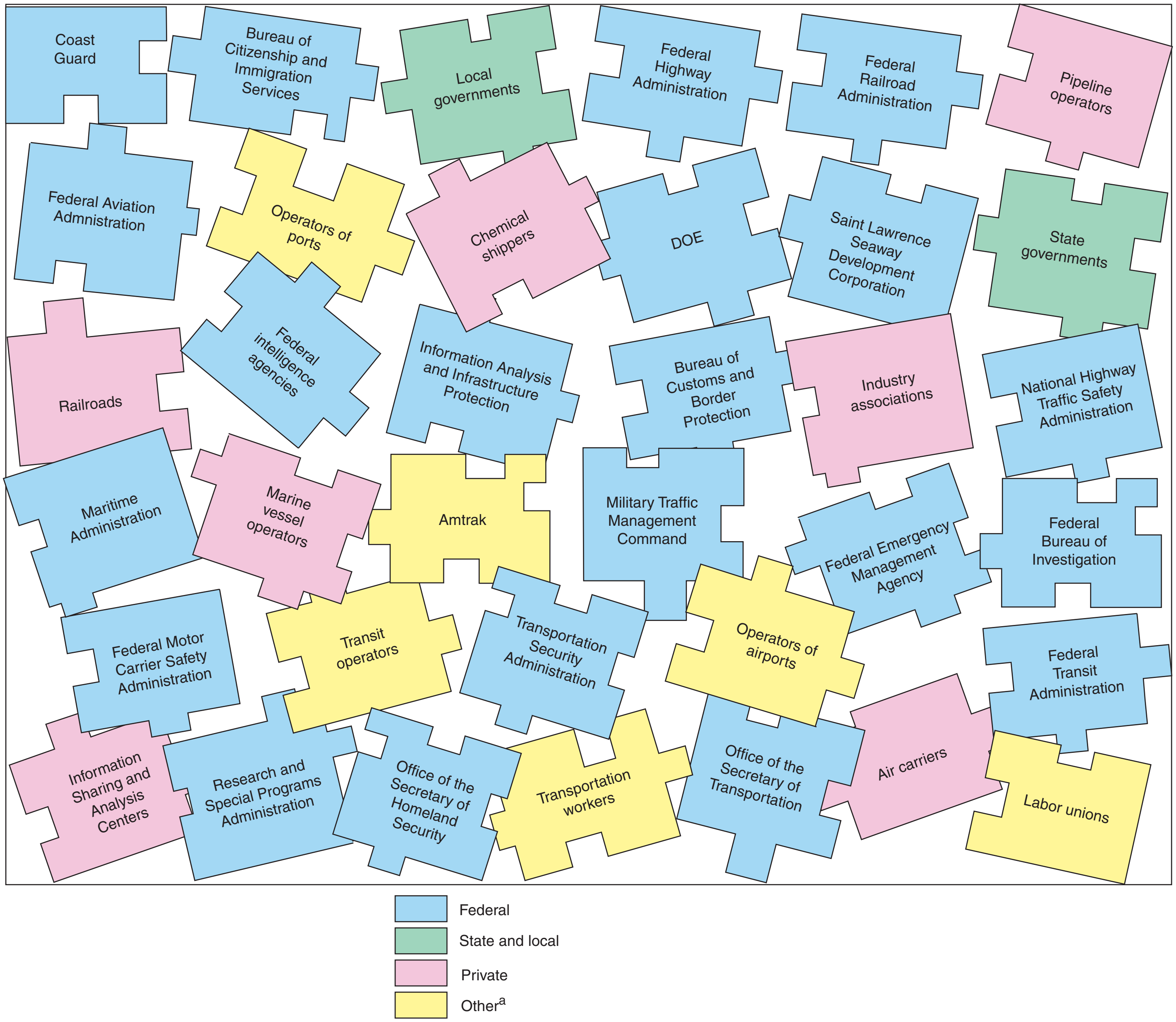
Interdependencies also exist between transportation and nearly every other sector of the economy. Consequently, an event that affects the transportation sector can have serious impacts on other industries. For example, when the war in Afghanistan began in October 2001, the rail industry stated that it 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. Additionally, the transportation system can be affected by other sectors. For example, representatives of the motor coach industry told us that the drop in the tourism industry has negatively affected motor coach profits.

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 4, 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;[10] 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.

[10] 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 4: Key Stakeholders in Transportation Security


Coast Guard
Bureau of Citizenship and Immigration Services
Local governments
Federal Highway Administration
Federal Railroad Administration
Pipeline operators
Federal Aviation Admnistration
Operators of ports
Chemical shippers
DOE
Saint Lawrence Seaway Development Corporation
State governments
Railroads
Federal intelligence agencies
Information Analysis and Infrastructure Protection
Bureau of Customs and Border Protection
Industry associations
National Highway Traffic Safety Administration
Maritime Administration
Marine vessel operators
Amtrak
Military Traffic Management Command
Federal Emergency Management Agency
Federal Bureau of Investigation
Federal Motor Carrier Safety Administration
Transit operators
Transportation Security Administration
Operators of airports
Federal Transit Administration
Information Sharing and Analysis Centers
Research and Special Programs Administration
Office of the Secretary of Homeland Security
Transportation workers
Office of the Secretary of Transportation
Air carriers
Labor unions
🟦 Federal
🟩 State and local
🟪 Private
🟨 Other[a]

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 is critical to successful implementation of security efforts.[11] 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 A 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. While 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 magnitude of the potential cost is illustrated by several examples:

- The President's fiscal year 2004 budget request for TSA includes about $4.5 billion for aviation security. According to TSA, this funding will be used for security screeners, air marshals, aviation related research and development, and surveillance detection techniques, among other things.

- The total estimated cost of the identified security improvements at eight mass transit agencies we visited was about $711 million.[12]

[11] See "Related GAO Products."

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

- The Coast Guard estimates the cost of implementing the new International Maritime Organization security code[13] and the security provisions in the Maritime Transportation Security Act of 2002[14] to be approximately $1.5 billion for the first year and $7.4 billion over the succeeding decade.

- The American Association of State Highway and Transportation Officials (AASHTO)[15] estimates that enhancing highway and transit security will cost $2 billion annually in capital costs and $1 billion in operating costs.

The current economic environment makes this a difficult time for the 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 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 are 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 this upcoming year. 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.

[13] The International Maritime Organization, an United Nations agency devoted exclusively to maritime matters, adopted international measures for port and shipping security in December 2002.

[14] P.L. No. 107-295, 116 Stat. 2064 (2002).

[15] AASHTO is a nonprofit, nonpartisan association representing highway and transportation departments in the 50 states, the District of Columbia, and Puerto Rico.

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.[16] However, as table 1 shows, the grant applications received by TSA for these security grants totaled $1.8 billion—7 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.

[16] 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 Transportation Security Grant Requests to 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. While 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."[17]

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

[17] *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 significant vulnerabilities remain, including: [18]

- **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 a background check. 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.

[18] See "Related GAO Products" at the end of this report for information on GAO reports that examine aviation security issues.

- **General aviation security:** While TSA has taken several actions related to general aviation[19] 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 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 who is 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 Florida teenage flight student crashed his single-engine airplane into a Tampa skyscraper.[20] 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, 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

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

[20] It should be noted that this event was not a terrorist attack.

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 consistency among motor coach operators in whether they remove their logos from the vehicles before they are sold. These vehicles could be used as a weapon or to transport a weapon. 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. The industry has been consistently operating at a heightened state of security since September 11. State and local governments have also made transportation security investments since September 11.

Transportation Operators Have Undertaken a Variety of Security-Enhancing Actions

According to representatives from a number of industry associations we interviewed,[21] transportation operators have implemented new security measures or increased the frequency or intensity of existing activities. Some of the most common measures cited include:

- **Conducted vulnerability or risk assessments:** Many transportation operators conducted assessments of their systems to identify potential vulnerabilities, critical infrastructure or assets, and corrective actions or needed security improvements. For example, the railroad industry conducted a risk assessment, that identified over 1,300 critical assets and served as a foundation for the industry's security plan.

- **Tightened access control:** Many transportation operators have tightened access control to their facilities and equipment by installing fences and requiring employees to display identification cards, among

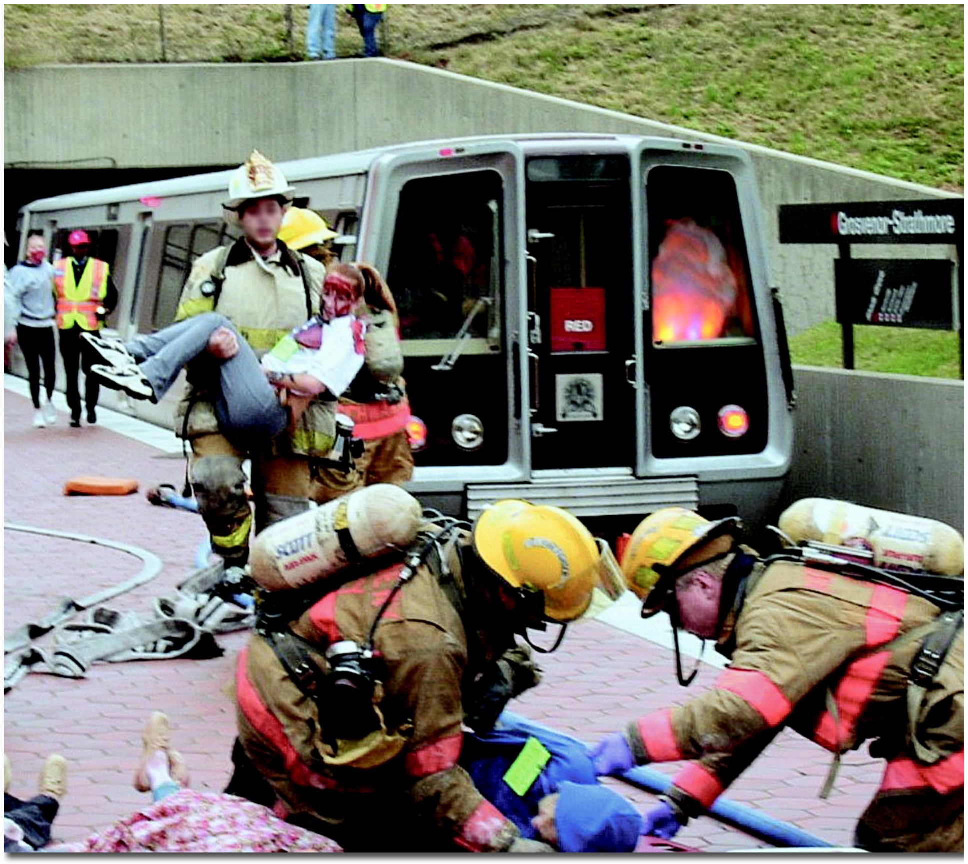
[21] Some of the industry associations we contacted include the American Bus Association, American Gas Association, American Trucking Associations, and Association of American Railroads. See appendix I for a complete list of industry associations we contacted.

other things. For example, some motor carrier operators have installed fences around truck yards and locked inventory at night.

- **Intensified security presence:** Some transportation operators have increased the number of police or security who patrol their systems. For example, transit agencies have placed surveillance equipment, alarms, or security personnel at access points to subway tunnels, bus yards, and other nonpublic places and required employees to wear brightly colored vests for increased visibility.

- **Increased emergency drills:** Many transportation operators have increased the frequency of emergency drills. For example, Amtrak reported that it has conducted two full-scale emergency drills in New York City and is currently trying to arrange a drill at Union Station in Washington, D.C. The purpose of emergency drilling is to test emergency plans, identify problems, and develop corrective actions. Figure 5 is a photograph from an annual emergency drill conducted by the Washington Metropolitan Area Transit Authority.

Figure 5: Emergency Drill in Progress



Source: GAO.

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

- **Developed or revised security plans:** Transportation operators developed security plans or reviewed existing plans to determine, what changes, if any, needed to be made. For example, DOT's Office of Pipeline Safety worked with the industry to develop performance oriented security guidance. The Office of Pipeline Safety also encouraged all pipeline operators to develop security plans and directed operators with critical facilities to develop security plans for these facilities.

- **Provided additional training:** Many transportation operators have either participated in and/or conducted additional training on security or antiterrorism. For example, the United Motorcoach Association is developing an online security training program for motor coach operators, using funds from the Intercity Bus Security Grant Program. Similarly, many transit agencies attended seminars conducted by FTA or by the American Public Transportation Association.

Some transportation industries have also implemented more innovative security measures, according to associations we contacted. For example, the natural gas industry modeled the impact of pipeline outages on the natural gas supply in the Northeast, which helped to identify vulnerabilities and needed improvements. The motor carrier industry developed a program called the Highway Watch Program, supported by the American Trucking Associations.[22] The program is a driver-led, state-organized safety system that since September 11 has included a security component. Specifically, drivers are provided terrorism awareness training and are encouraged to report suspicious activities they witness on the road to a Highway Watch Program call center, which is operated 24 hours a day, 7 days a week. The call center then directs the call to appropriate authorities.

State and Local Governments Have Also Increased Security-Related Efforts

As we have previously reported, state and local governments are critical stakeholders in the nation's homeland security efforts.[23] 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 to state and local governments.

[22] The Highway Watch Program is funded by a $500,000 grant from the Federal Motor Carrier Safety Administration.

[23] See "Related GAO Products" at the end of this report.

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 additional law enforcement officers and overtime.

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

The Congress, DOT, TSA, and other federal agencies, took 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),[24] Congress passed numerous pieces of legislation aimed at improving transportation security. For example, Congress passed the USA PATRIOT Act of 2001,[25] which mandates federal background checks of individuals operating vehicles carrying hazardous materials and the Homeland Security Act,[26] which created DHS and moved TSA to the new department.[27] Congress also provided funding for transportation security enhancements through various appropriations acts.

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

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

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

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. (See app. IV for a listing of the key pieces of transportation security-related legislation that has been passed since September 11.)

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.[28] According to TSA, other completed TSA activities included the following:

- 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 security of air, land,

[27] 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.

[28] 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.

and maritime transportation. As table 2 shows, the actions taken by DOT modal administrations varied. For example, FTA launched a multipart initiative for mass transit agencies, which 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 response of various DOT modal agencies to the threat of terrorist attacks on the transportation system has varied due to differences in authority and resource limitations.

Table 2: Key Actions Taken By DOT Modal Administrations to Secure the Different Transportation Modes, 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.
Maritime	U.S. Coast Guard[a]	• 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 Guards' National Strike Force to prepare for and respond to bioterrorism and weapons of mass destruction.
	Maritime Administration	• 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.

(Continued From Previous Page)

Mode	DOT modal administration	Examples of actions taken
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.
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 email 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 largest 36 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)).

In addition to TSA and DOT modal administrations, other federal agencies have also taken actions to improve security.[29] For example, the Bureau of

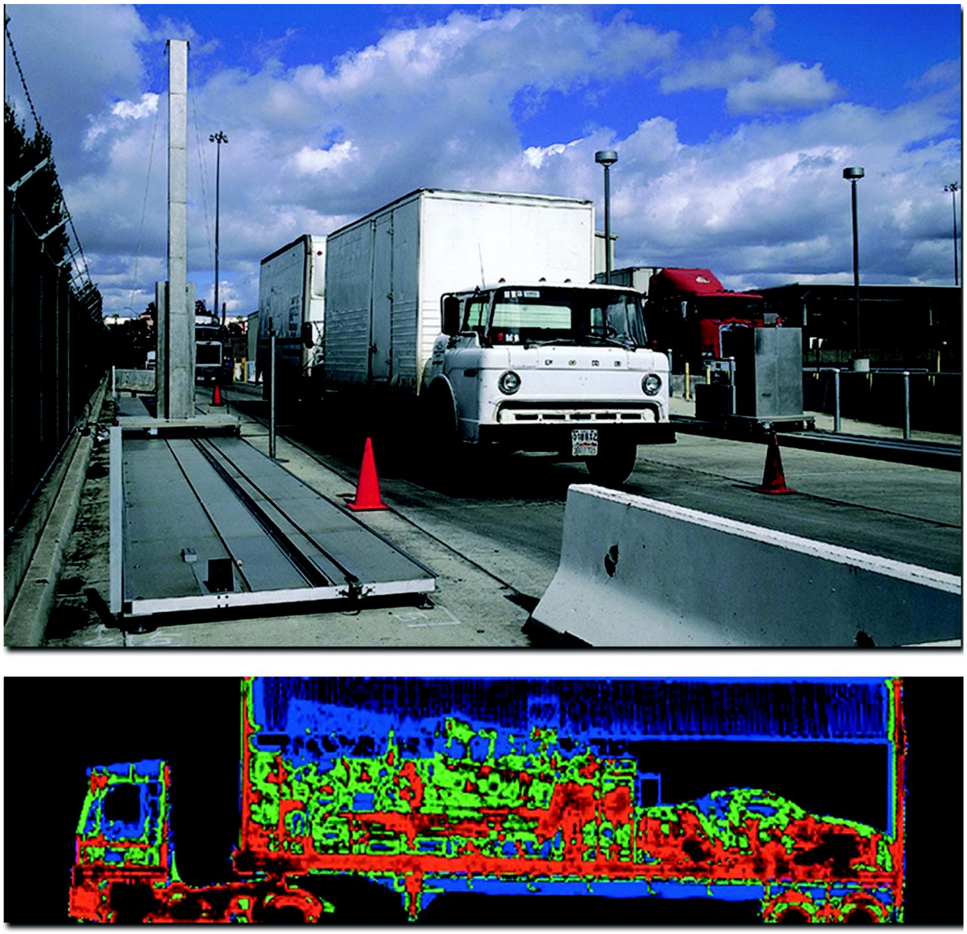
[29] See appendix IV for highlights of final regulations issued since September 11 that govern transportation security.

Customs and Border Protection (CBP), previously known as the U.S. Customs Service, has played a key role in improving port security.[30] Since September 11, the agency has launched a number of initiatives to strengthen the security of the U.S. border, including ports. The initiatives are part of a multilayered approach, which rely on partnerships between foreign nations and the U.S. to identify problems at their source, cooperation from the global trade community to secure the flow of goods, and collaboration between federal, state, and local law enforcement and intelligence agencies to ensure that information is analyzed and used to target scarce resources on the highest risk issues. Some of the specific initiatives that CBP has implemented to interdict high risk cargo before it reaches the U.S. include the following:

- Developing and deploying of a strategy for the detection of nuclear and radiological weapons and materials. The elements of this strategy—equipment, training, and intelligence—are focused on providing inspectors with the tools to detect weapons of mass destruction in cargo containers and vehicles. In the maritime environment, this includes the deployment of radiation portal monitors, personal radiation detectors, large-scale nonintrusive inspection technology, such as truck and container x-rays and mobile x-ray vans. Much of the development of this equipment has been done in partnership with the Department of Energy. Figure 6 shows new mobile gamma ray imaging devices at ports to help inspectors examine the contents of cargo containers and vehicles.

[30] 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.

Figure 6: Photograph of Inspection Equipment in Use



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

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.

- 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. According to CBP, this initiative has leveraged the cooperation of the owners of the global supply chain by working with this community to implement and share standard security best practices. The members of C-TPAT include importing businesses, freight forwarders, carriers, and U.S. port authorities and terminal operators. According to CBP, C-TPAT members bring 96 percent of all containers coming into the U.S. After the initial application and training phase of this program, CBP conducts foreign and domestic validations to verify that the supply chain security measures contained in C-TPAT participants' security profiles are reliable, accurate, and effective. C-TPAT members are strongly encouraged to self-police such areas as personnel screening, physical security procedures and personnel, and the security of service providers.

- Launching the Container Security Initiative (CSI), which is designed specifically to secure the ocean-going sea container. The key elements of CSI include using advance information to identify high-risk containers; inspecting containers identified through the prescreening process as high-risk before they are shipped to the U.S.; using detection technology to quickly inspect containers identified as high-risk; and developing and using smarter, more secure containers. According to CBP, the U.S. has signed agreements with 18 of the countries with the world's largest seaports, which allows for the deployment of U.S. inspectors and equipment to these foreign seaports, and is beginning the expansion of CSI to other global ports with significant volume or strategic locations.

TSA Moves Forward as Its Role in Transportation Security Evolves

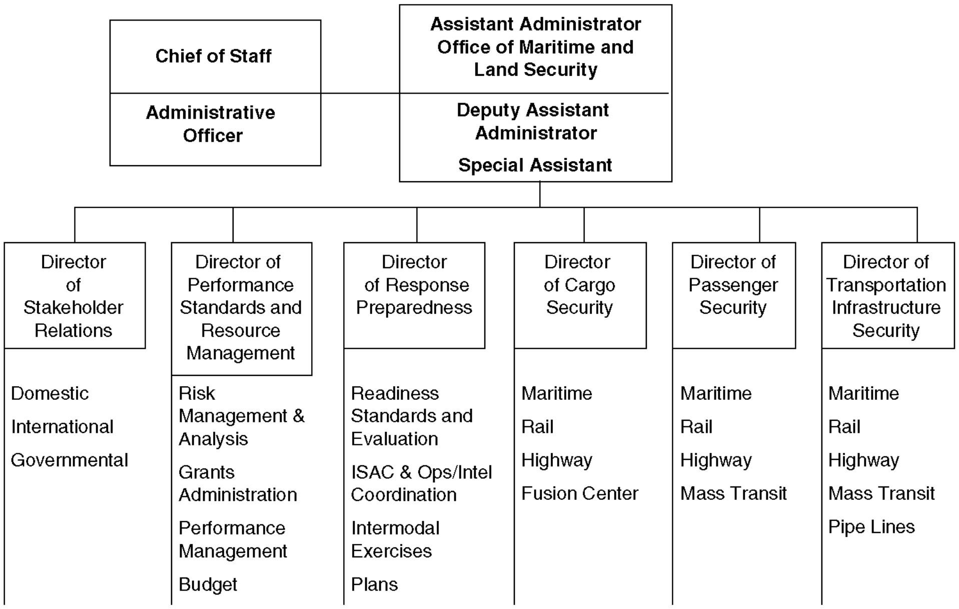
TSA is moving forward with efforts to secure the entire transportation system. TSA has adopted a systems approach—that is, a holistic rather than a modal approach—to securing the transportation approach. In addition, TSA is using risk management principles to guide its decision-making. To help TSA make risk-based decisions, TSA is developing standardized criticality, threat, and vulnerability assessment tools. 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 to Securing All Modes of Transportation

TSA is taking a systems approach to securing the transportation system. Using this 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 others. 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.

The systems approach is reflected in the organizational structure of TSA’s Office of Maritime and Land Security, which is responsible for the security of the maritime and land modes of transportation. Rather than organize around the different modes of transportation, such as DOT’s modal administrations, the office is organized around cross-modal issues. As figure 7 shows, the Office of Maritime and Land Security has six divisions, including Cargo Security and Passenger Security. The director of each division will be responsible for a specific aspect of security of multiple modes. For example, the Director of Cargo Security will be responsible for cargo security for all surface modes of transportation.

Figure 7: Organizational Chart of TSA's Office of Maritime and Land Security, June 2003


Chief of Staff
Administrative Officer
Assistant Administrator Office of Maritime and Land Security
Deputy Assistant Administrator
Special Assistant
Director of Stakeholder Relations
Domestic
International
Governmental
Director of Performance Standards and Resource Management
Risk Management & Analysis
Grants Administration
Performance Management
Budget
Director of Response Preparedness
Readiness Standards and Evaluation
ISAC & Ops/Intel Coordination
Intermodal Exercises
Plans
Director of Cargo Security
Maritime
Rail
Highway
Fusion Center
Director of Passenger Security
Maritime
Rail
Highway
Mass Transit
Director of Transportation Infrastructure Security
Maritime
Rail
Highway
Mass Transit
Pipe Lines

Source: TSA.

Note: See appendix V to view the organizational chart for TSA and where the Office of Maritime and Land Security is located within the organization.

TSA Applies Risk Management Principles

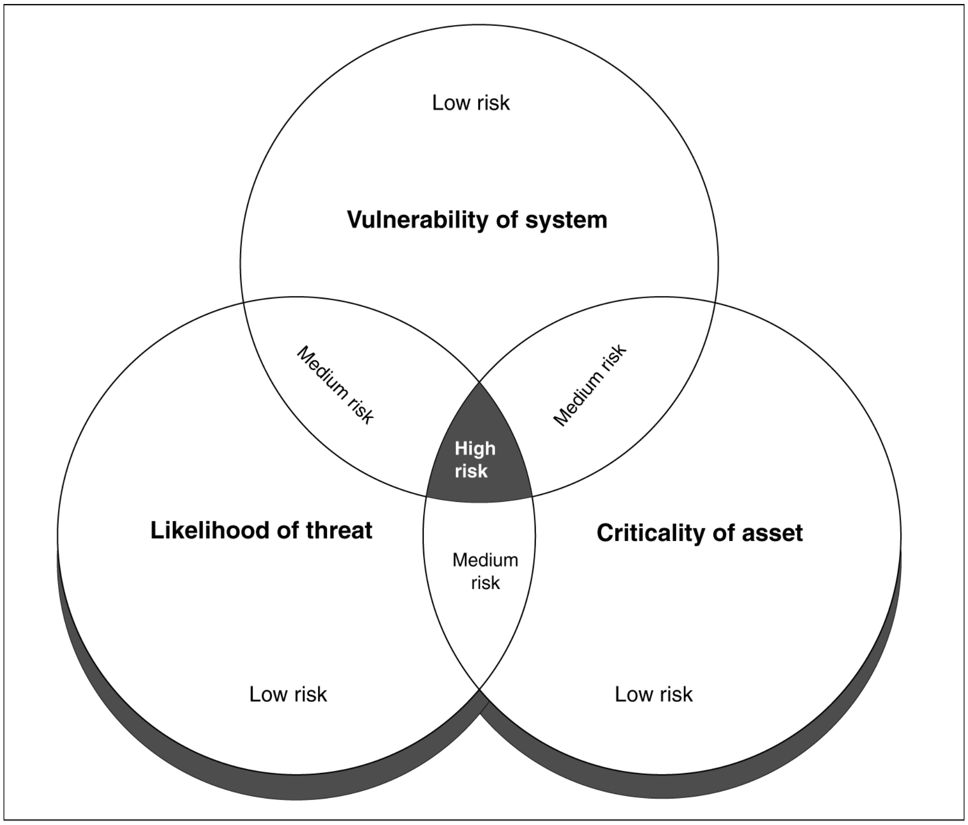
TSA has adopted a risk management approach for its efforts to enhance the security of the nation's transportation system. A risk management approach is a systematic process to analyze threats, vulnerabilities, and the criticality (or relative importance) of assets to better support key decisions in order to link resources with prioritized efforts. Table 3 describes this approach. As figure 8 illustrates, 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 at most 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.

Table 3: Elements of a Risk Management Approach

A **threat assessment** identifies and evaluates potential threats on the basis of factors such as capabilities, intentions, and past activities. This assessment represents a systematic approach to identifying potential threats before they materialize. However, even if updated often, a threat assessment might not adequately capture some emerging threats. The risk management approach, therefore, uses vulnerability and criticality assessments as additional input to the decision-making process.
A **vulnerability assessment** identifies weaknesses that may be exploited by identified threats and suggests options to address those weaknesses.
A **criticality assessment** evaluates and prioritizes assets and functions in terms of specific criteria, such as their importance to public safety and the economy. The assessment provides a basis for identifying which structures or processes are relatively more important to protect from attack. As such, it helps managers to determine operational requirements and target resources to the highest priorities while reducing the potential for targeting resources to lower priorities.

Source: GAO.

Figure 8: Illustration of How Risk Management Approach Can Guide Decision-Making



Source: GAO.

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 all assets from being equally protected; 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.

Other transportation stakeholders are also using risk management principles. For example, the rail industry conducted a comprehensive risk analysis of its infrastructure, which included an assessment of threats, vulnerabilities, and criticality. The results of the risk analysis formed the basis for the rail industry's security management plan, which identified countermeasures for the different threat levels. Similarly, the pipeline industry is using a risk management approach in securing its infrastructure. The Office of Pipeline Safety and industry associations noted that the pipeline industry had adopted a risk management approach for safety prior to September 11. As a result, the industry extended this approach to its security efforts after September 11.

TSA Is Developing Standard Assessment Tools to Help Make Risk-Based Decisions

To help TSA make risk based decisions, TSA's Office of Threat Assessment and Risk Management is developing two assessment tools that will help assess threats, criticality, and vulnerabilities. The first tool will assess the criticality of a transportation asset or facility. TSA is working with DHS' Information Analysis and Infrastructure Protection (IAIP) Directorate to ensure that TSA's criticality tool will be consistent with the IAIP's approach for managing critical infrastructure. TSA's criticality tool will incorporate multiple factors, such as fatalities, economic importance, and socio-political importance, to arrive at a criticality score. The score will enable TSA, in conjunction with transportation stakeholders, to rank assets and facilities within each mode. According to TSA, by identifying and prioritizing assets and facilities, TSA can focus resources on that which is deemed most important.

The second tool is referred to as the Transportation Risk Assessment and Vulnerability Evaluation Tool (TRAVEL). This tool will assess threats and analyze vulnerabilities for all transportation modes. According to TSA officials, TSA has worked with a number of organizations in developing TRAVEL, including the Department of Defense, Sandia National Laboratories, and AASHTO. TSA is also working with economists on developing the benefit/cost component of this model. TSA officials believe that a standard threat and vulnerability assessment tool is needed so that TSA can identify and compare threats and vulnerabilities across the modes. If different methodologies are used in assessing the threats and vulnerabilities, comparisons can be problematic. A standard assessment tool would ensure consistent methodology. Using TRAVEL, TSA plans to gather comparable threat and vulnerability information across all modes of transportation, which would inform TSA's risk-based decision-making.

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. TSA plans to begin rolling out the standards starting summer 2003.[31]

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

- **Standards will be performance-based**. Rather than prescriptive standards, TSA standards will be performance-based, which will allow transportation operators to determine how best to achieve the desired level of security. TSA officials believe that performance-based standards

[31] The Information Analysis and Infrastructure Protection Directorate within DHS is working with TSA, 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 Coast Guard's significant role in securing maritime transportation, TSA will likely play a coordination role in the maritime arena.

provide for operator flexibility, allow for 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 have not 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 it could alter their relationships with the industry. Historically, DOT surface transportation modal administrations' missions 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 on 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, to staff or funding to enforce new security standards.

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 is also necessary. However, achieving such consensus and compromise may be difficult, given the conflicts between some stakeholders' goals and interests.

Stakeholders Are Concerned About Pending Standards

Transportation stakeholders expressed concerns about TSA's plan to issue mandatory security standards for all modes of transportation. A common concern raised by associations was that standards represent unfunded mandates, unless the federal government pays for the standards that it promulgates. 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. TSA officials said they hope to provide grants to implement the standards; however, it is unclear at this time if grants will be available.

Another common concern expressed by transportation security experts and industry associations is that TSA does not have the necessary expertise or knowledge to develop appropriate security standards for the industry. In a 2003 report to Congress, TSA recognizes that each transportation mode has unique characteristics that make various security measures more or less feasible or appropriate.[32] However, a number of industry associations, transportation security experts, and DOT modal administrations expressed concern that TSA does not have a good understanding of the unique challenges of the modes, such as the need to maintain accessibility in transit systems, or the possible negative ramifications—both operationally and financially—of standards. Officials from one DOT modal administration noted that industry representatives left a meeting with TSA officials with serious concerns regarding TSA officials' understanding of their industry. Senior TSA officials stated that TSA employees have extensive subject matter expertise in transportation and security issues. Moreover, TSA officials stated that they will draw on the expertise and knowledge of the transportation industry and other DHS agencies, such as the Coast Guard, as well as all stakeholders in developing the standards.

A number of representatives from industry associations also expressed concerns that TSA may issue mandatory or regulatory standards, especially since their industries have taken proactive steps to enhance security since September 11. Industry associations also noted that the majority of transportation infrastructure in some modes is privately owned. As such, transportation operators have an economic incentive to ensure the security of their infrastructure; hence, operators are voluntarily implementing increased security measures. For example, the pipeline industry worked with DOT's Office of Pipeline Safety to develop industry-wide security guidelines. These guidelines are risk-based and identify countermeasures that pipeline operators should implement at different threat levels. The pipeline guidelines are also voluntary. According to pipeline industry associations, the pipeline industry is implementing these security guidelines. Representatives from industry associations stated that TSA should wait to see if industry-developed, voluntary measures are working before issuing mandatory standards. TSA officials noted that 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 before issuing mandatory standards.

Finally, industry representatives 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

[32] Transportation Security Administration, *Report to Congress on Transportation Security*, (March 31, 2003).

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. TSA officials repeatedly told us they understand the importance of gaining stakeholder buy-in and partnering with the industry. They also stated that they have conducted outreach to transportation stakeholders and plan to continue their outreach efforts in the future. TSA is developing a strategy that will serve as its framework for communicating with transportation stakeholders and obtaining stakeholders' input in TSA's decision-making. TSA plans to finalize this strategy in July 2003.

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 that 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 current initiatives 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. FTA's goal is to have the largest 30 agencies implement at least 80 percent of these measures by the end of fiscal year 2003.

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 the computer systems. The air traffic control system's computers help the nation's air traffic controllers 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.[33] 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 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

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

eliminate DOT modal administrations' existing statutory responsibilities for securing 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 were planning to develop memorandums of agreement. The purpose of these documents was to define the roles and responsibilities of the different agencies as they relate to 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. 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, with the exception of the memorandum of agreement between FAA and TSA, the draft memorandums were very generic and did not provide much clarification. Consequently, DOT and TSA decided not to execute or sign the memorandums of agreement, except for the memorandum of agreement between FAA and TSA, which was signed on February 28, 2003.[34]

The General Counsel suggested several reasons why the majority of 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 is 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

[34] 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.

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 they would be open to using memorandums of agreement in the future.

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, should be implemented 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. The experts and representatives generally believe that these actions are the responsibility of the federal government.

Clear federal roles and responsibilities is a core issue in transportation security, according to transportation experts and associations that we contacted. The lack of clarity about the roles and responsibilities of federal actors 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 associations stated that their members were unclear of which agency to contact for their various security concerns and which agency has oversight for certain issues. Furthermore, 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 among the industry. They said the uncertainty about federal roles and the lack of coordination is 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.

According to transportation experts and associations we contacted, a national transportation strategy is essential to moving forward with transportation security. It 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,[35] which according to the Deputy Administrator of TSA, will provide an overarching framework for the security of all modes.

Transportation security experts and association representatives we contacted believe that the federal government should provide funding for needed security improvements. While an overall security strategy is a prerequisite to investing wisely, providing adequate funding also is essential. 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 these standards will be considered unfunded mandates that the industry and state and local governments have to absorb.

The federal government needs to play a strong role in investing in and setting a research and development agenda for transportation security, according to most transportation security experts and associations we contacted. They view this as an appropriate role for the federal government, since 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

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

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.

Transportation security experts and representatives from state and local government and industry associations stated that the federal government needs to play a vital role in sharing information—specifically, intelligence information and related guidance. Representatives from numerous associations commented that the federal government needs to provide timely, localized, actionable intelligence information. 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 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.

Conclusions

During TSA’s first year of existence, TSA met a number of challenges, including successfully meeting many congressional deadlines for aviation security. With the immediate crisis of meeting key aviation security deadlines behind TSA, it 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.

Recommendation for Executive Action

To clarify and define the roles and responsibilities of TSA and DOT modal administrations in transportation security matters, we recommend that the Secretary of Transportation and Secretary of Homeland Security use a mechanism, such as a memorandum of agreement to clearly delineate their roles and responsibilities. At a minimum, this mechanism should establish the responsibilities of each entity in setting, administering, and implementing security standards and regulations, determining funding priorities, and interfacing with the transportation industry as well as define each entity's role in the inevitable overlap of some safety and security activities. After the roles and responsibilities of each entity are clearly defined, this information should be communicated to all transportation stakeholders.

Agency Comments

We provided DOT, DHS, and Amtrak with a draft of this report for review and comment. Amtrak generally agreed with our findings and recommendation and provided some technical comments, which we have incorporated into this report where appropriate.

DOT and DHS generally agreed with the report's findings. However, they disagreed with the conclusion and recommendation that their roles and responsibilities need to be clarified and defined. The two departments stated that the roles and responsibilities of each entity is clear—that is, DHS has primary responsibility for transportation security and DOT will play a supporting role in such matters. We agree that the Aviation and Transportation Security Act[36] (ATSA) gave TSA primary responsibility for securing all modes of transportation. However, neither this act, nor other legislation defined TSA's roles and responsibilities in securing all modes of transportation. Specifically, 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. The act also did not eliminate DOT modal administrations' existing statutory responsibilities for securing the different modes of transportation. Moreover, recent legislation clarifies that DOT still has transportation 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.

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

In addition, although DOT and DHS believe their roles and responsibilities are clearly defined, transportation security stakeholders we contacted are not as certain. 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. Representatives from several associations also told us that their members are receiving different messages from the various federal agencies involved in transportation security.

Furthermore, as noted in the report, both TSA and DOT are moving forward with transportation security efforts. As both entities continue with their security efforts, it is important that the roles and responsibilities of each entity are coordinated and clearly defined. The lack of clarity can lead to duplication, confusion, and/or gaps in preparedness. We therefore continue to recommend that DOT and DHS use a mechanism, such as a memorandum of agreement, to clarify and define DOT modal administration's and TSA's roles and responsibilities in transportation security. After the roles and responsibilities of each entity are clearly defined, this information should be communicated to all transportation stakeholders.

DOT and DHS also noted that the title of the draft report, *Transportation Security: More Federal Coordination Needed to Help Address Security Challenges*, as well as our conclusions and recommendations place too much emphasis on coordination. To better capture our conclusions and recommendations—that is, that the roles and responsibilities of TSA and DOT in security matters should be clearly delineated and communicated to all transportation security stakeholders—we have changed the report's title to *Transportation Security: Federal Action Needed to Help Address Security Challenges*. However, we disagree that the report places too much emphasis on the lack of coordination between DOT and DHS. As noted above, representatives from several associations told us that their members have received conflicting messages from the federal agencies involved in transportation security. Moreover, there appears to be a break down in communication between TSA and DOT about current security initiatives. For example, although TSA officials stated that they have informed DOT about their plans to issue security standards, some DOT officials we met with were unsure as to whether TSA was issuing standards, what the standards would entail, or the time frames for issuing the standards.

In addition to their written comments, DHS and DOT provided technical comments to our draft, which we have incorporated into the report where appropriate.

See appendixes II and III for DOT's and DHS' comments and our responses.

As we agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. We will then send copies of this report to the Secretary of Transportation, the Secretary of Homeland Security, the Administrator of the Transportation Security Administration, the President and Chief Executive Officer of Amtrak, the Director of the Office of Management and Budget, and interested congressional committees. We will make copies available to others upon request. In addition, this report will be available at no charge on our Web site at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me on (202) 512-2834 or at guerrerop@gao.gov. Individuals making key contributions to this report are listed in appendix VI.

Peter Guerrero
Director, Physical Infrastructure Issues

List of Requesters

The Honorable John McCain
Chairman
Committee on Commerce,
Science, and Transportation
United States Senate

The Honorable Ernest Hollings
Ranking Minority Member
Committee on Commerce,
Science, and Transportation
United States Senate

The Honorable James Jeffords
Ranking Minority Member
Committee on Environment and
Public Works
United States Senate

The Honorable Harry Reid
Ranking Minority Member
Subcommittee on Transportation
and Infrastructure
Committee on Environment and
Public Works
United States Senate

The Honorable Thomas Carper
United States Senate

The Honorable Hillary Rodham Clinton
United States Senate

The Honorable Kay Bailey Hutchison
United States Senate

The Honorable Gordon Smith
United States Senate

Scope and Methodology

To address our four objectives, we conducted structured interviews with officials from TSA, Amtrak, and DOT, representatives from the major transportation industry associations and state and local government associations, and select transportation security experts. We selected transportation security experts based on their knowledge/expertise and reputation as being an expert in the transportation security arena. We also consulted with the National Academy of Sciences in identifying appropriate transportation security experts. Table 4 shows the federal agencies, industry associations, transportation security experts, and state and local government associations that were interviewed. Through these structured interviews we collected information on the challenges that exist in securing the transportation system, vulnerabilities of different modes, actions that transportation stakeholders—including the federal, state, and local governments and the operators—have taken to enhance security since September 11, TSA's and DOT's ongoing and planned security efforts, roles and responsibilities of TSA and DOT in securing the transportation system, and future security actions that industry associations and security experts believe are needed. We synthesized and analyzed the information from the structured interviews.

Table 4: List of Interviewees

Federal agencies
Amtrak
Department of Transportation (DOT)
General Counsel
Intermodal Hazardous Materials Program
Office of Emergency Transportation
Office of the Secretary of Transportation (OST)
Federal Aviation Administration (FAA)
Office of the Chief Information Officer
Office of Security and Investigations (ASI)
Federal Highway Administration (FHWA)
Federal Motor Carrier Safety Administration (FMCSA)
Federal Railroad Administration (FRA)
Federal Transit Administration (FTA)
Office of Pipeline Safety (OPS)
Transportation Security Administration (TSA)
Assistant Administrator for Aviation Operations

(Continued From Previous Page)

Chief Financial Officer (CFO)
Office of Maritime and Land Security
Office of Policy (Aviation)
Risk Management/Strategic Planning
Support Systems Directorate
United States Coast Guard
Industry associations
Air Transport Association (ATA)
American Association of Airport Executives (AAAE)
American Bus Association (ABA)
American Gas Association (AGA)
American Petroleum Institute (API)
American Road and Transportation Builders Association (ARTBA)
American Trucking Associations (ATA)
Association of Oil Pipelines (AOPL)
Association of American Railroads (AAR)
Commercial Vehicle Safety Alliance (CVSA)
Consolidated Safety Services (CSS)
Interstate Natural Gas Association of America (INGAA)
National Academy of Sciences (NAS)
National Association of Regulatory Utility Commissioners (NARUC)
National Private Truck Council (NPTC)
United Motorcoach Association (UMA)
Transportation security experts
Annabelle Boyd, President and Senior Consultant, Boyd, Caton & Grant Transportation Group, Inc.
Mortimer L. Downey III, PB-Consult, Inc.
Stephen E. Flynn, Ph.D., Jeane J. Kirkpatrick Senior Fellow in National Security Studies, Council on Foreign Relations
Yacov Y. Haimes, Director, Center for Risk Management of Engineering Systems, University of Virginia
Arnold M. Howitt, Ph.D., Executive Director, Taubman Center for State and Local Government, Director, Executive Session on Domestic Preparedness, Kennedy School of Government, Harvard University
Brian M. Jenkins, Senior Advisor to the President, RAND Corporation
Douglas R. Laird, Principal, Laird & Associates, Inc.
James Wilding, Executive Director (Retired), Metropolitan Washington Airport Authority
State and local government associations
American Association of State Highway and Transportation Officials (AASHTO)
National Association of Counties (NACO)

(Continued From Previous Page)
National Emergency Management Association (NEMA)
National League of Cities (NLC)

Source: GAO.

In addition to the structured interviews, we analyzed the administration's *National Strategy for Homeland Security* and the *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* and the Federal Bureau of Investigation's *The Terrorist Threat to the U.S. Homeland: An FBI Assessment*. We also reviewed current transportation security-related research as well as transportation security-related reports and documents from TSA, Amtrak, and DOT, including strategic planning documents, memorandums, program descriptions, and budget and financial documents. We also analyzed security-related documents from industry associations, including action plans, operational information, and reports, and the U.S. Code and the Code of Federal Regulations. We also incorporated the findings of previous GAO reports on port, transit, aviation, and homeland security.[1]

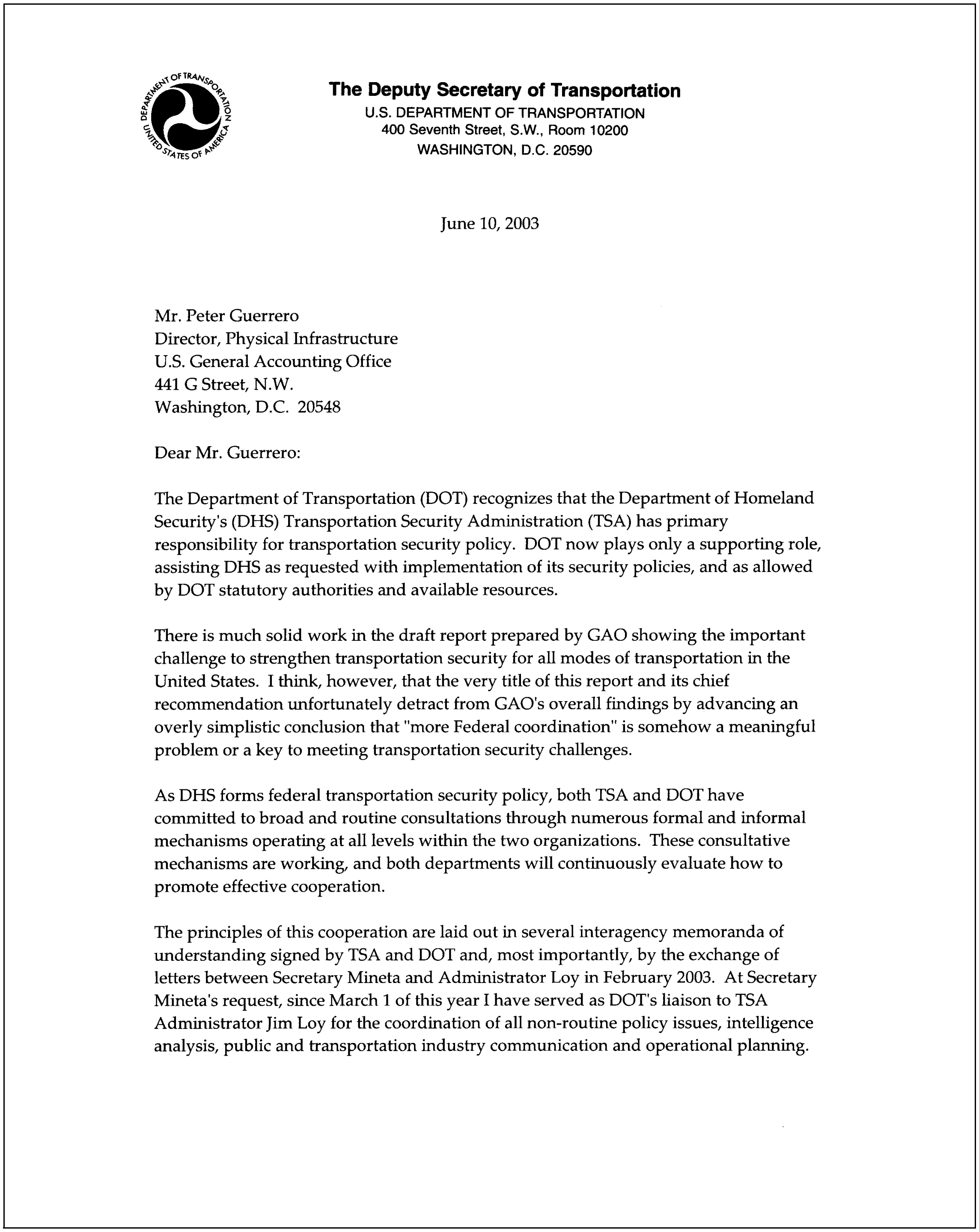
We conducted our work from February 2003 through May 2003, in accordance with generally accepted government auditing standards.

[1] In preparing these previous reports, we contacted numerous transportation security stakeholders, including transit agencies, port authorities, and local and state governments as well as representatives from the chemical and maritime industries. We also contacted various federal departments including the Departments of Defense, Energy, Homeland Security, Justice, and Health and Human Services.

Appendix II

Comments from the Department of Transportation

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



The Deputy Secretary of Transportation
U.S. DEPARTMENT OF TRANSPORTATION
400 Seventh Street, S.W., Room 10200
WASHINGTON, D.C. 20590

June 10, 2003

Mr. Peter Guerrero
Director, Physical Infrastructure
U.S. General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Guerrero:

The Department of Transportation (DOT) recognizes that the Department of Homeland Security's (DHS) Transportation Security Administration (TSA) has primary responsibility for transportation security policy. DOT now plays only a supporting role, assisting DHS as requested with implementation of its security policies, and as allowed by DOT statutory authorities and available resources.

See comment 1.

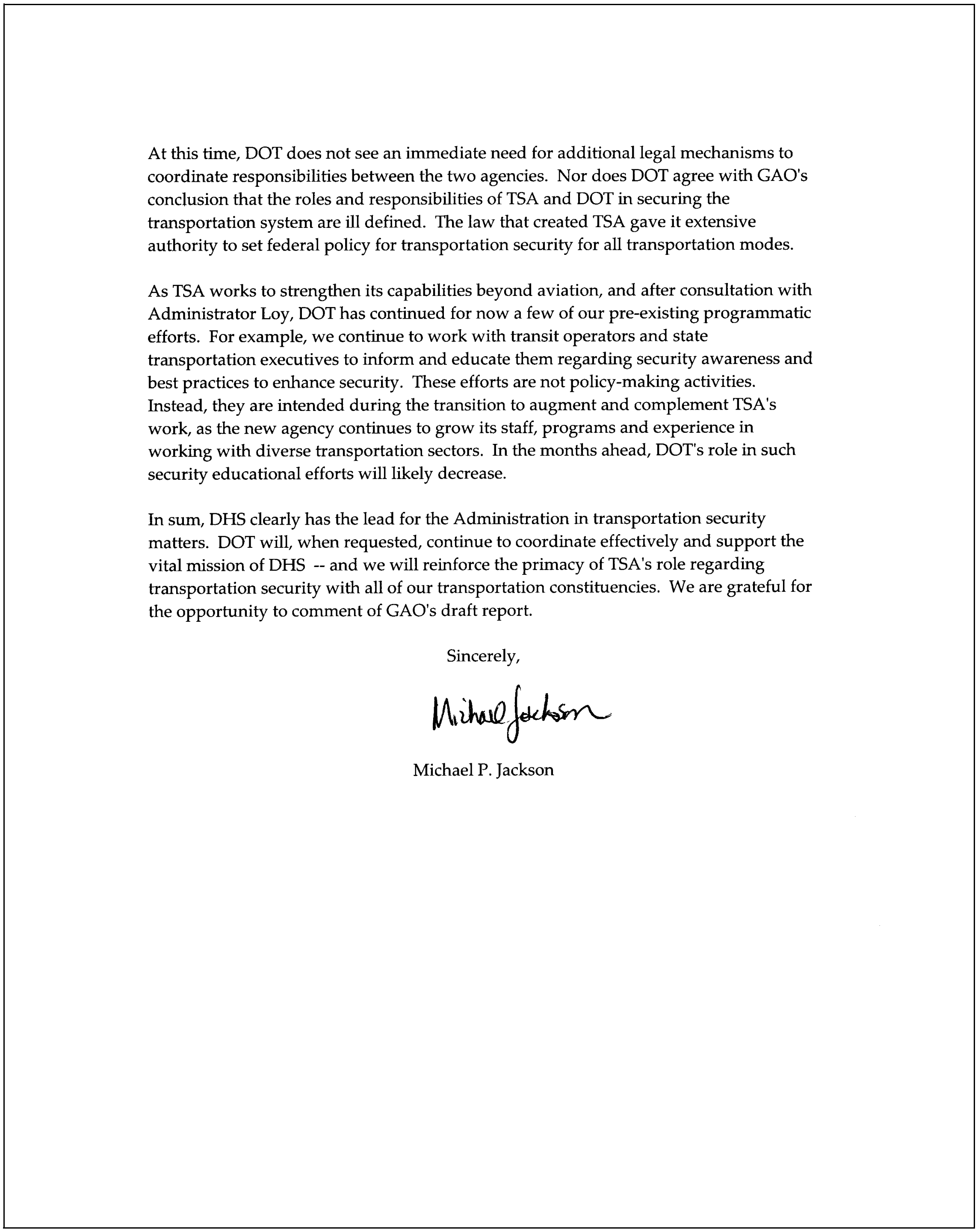
There is much solid work in the draft report prepared by GAO showing the important challenge to strengthen transportation security for all modes of transportation in the United States. I think, however, that the very title of this report and its chief recommendation unfortunately detract from GAO's overall findings by advancing an overly simplistic conclusion that "more Federal coordination" is somehow a meaningful problem or a key to meeting transportation security challenges.

See comment 2.

As DHS forms federal transportation security policy, both TSA and DOT have committed to broad and routine consultations through numerous formal and informal mechanisms operating at all levels within the two organizations. These consultative mechanisms are working, and both departments will continuously evaluate how to promote effective cooperation.

See comment 3.

The principles of this cooperation are laid out in several interagency memoranda of understanding signed by TSA and DOT and, most importantly, by the exchange of letters between Secretary Mineta and Administrator Loy in February 2003. At Secretary Mineta's request, since March 1 of this year I have served as DOT's liaison to TSA Administrator Jim Loy for the coordination of all non-routine policy issues, intelligence analysis, public and transportation industry communication and operational planning.



See comment 4.

At this time, DOT does not see an immediate need for additional legal mechanisms to coordinate responsibilities between the two agencies. Nor does DOT agree with GAO's conclusion that the roles and responsibilities of TSA and DOT in securing the transportation system are ill defined. The law that created TSA gave it extensive authority to set federal policy for transportation security for all transportation modes.

See comment 5.

As TSA works to strengthen its capabilities beyond aviation, and after consultation with Administrator Loy, DOT has continued for now a few of our pre-existing programmatic efforts. For example, we continue to work with transit operators and state transportation executives to inform and educate them regarding security awareness and best practices to enhance security. These efforts are not policy-making activities. Instead, they are intended during the transition to augment and complement TSA's work, as the new agency continues to grow its staff, programs and experience in working with diverse transportation sectors. In the months ahead, DOT's role in such security educational efforts will likely decrease.

In sum, DHS clearly has the lead for the Administration in transportation security matters. DOT will, when requested, continue to coordinate effectively and support the vital mission of DHS -- and we will reinforce the primacy of TSA's role regarding transportation security with all of our transportation constituencies. We are grateful for the opportunity to comment of GAO's draft report.

Sincerely,

Michael Jackson

Michael P. Jackson

The following are GAO's comments on the Department of Transportation letter dated June 10, 2003.

GAO Comments

1. We agree that the title of the report should be changed. Our conclusions and recommendation call for the roles and responsibilities of TSA and DOT in security matters to be clearly delineated and communicated to all transportation security stakeholders. To more fully capture our conclusions and recommendations, we have changed the report's title to *Transportation Security: Federal Action Needed To Help Address Security Challenges*.

   However, we disagree that our recommendation advances an "overly simplistic conclusion that 'more Federal coordination' is somehow a meaningful problem or a key to meeting transportation security challenges." Although coordination does not solve all security challenges, it is a key element in meeting transportation security challenges. As we have noted in previous reports, coordination among all levels of the government and the private industry is critical to the success of security efforts. The lack of coordination can lead to problems such as duplication and/or conflicting efforts, gaps in preparedness, and confusion. Moreover, the lack of coordination can strain intergovernmental relationships, drain resources, and raise the potential for problems in responding to terrorism. The administration's *National Strategy for Homeland Security* and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* also emphasize the importance of and need for coordination in security efforts. In particular, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* notes that protecting critical infrastructure, such as the transportation system, "requires a unifying organization, a clear purpose, a common understanding of roles and responsibilities, accountability, and *a set of well-understood coordinating processes*." (Italics added for emphasis.)

2. We disagree that the commitment of TSA and DOT to broad and routine consultations through numerous formal and informal mechanisms is working. As we noted throughout the report, representatives from several associations told us that they have received conflicting messages from the federal agencies involved in transportation security. Representatives from several associations also 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.

Moreover, there appears to be a break down in communication between TSA and DOT about current security initiatives. For example, although TSA officials stated that they have informed DOT about their plans to issue security standards, some DOT officials we met with were unsure as to whether TSA was issuing standards, what the standards would entail, or the time frames for issuing the standards.

3. We do not believe the correspondence exchanged by Secretary Mineta and Admiral Loy adequately defines the roles and responsibilities of TSA and DOT in security issues. Rather than delineate the roles and responsibilities of each entity in security matters, such as determining funding priorities and interfacing with stakeholders, the correspondence primarily 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 the Federal Aviation Administration (FAA) as a framework for their interactions on security matters for all other modes. Given the complexities and unique challenges in securing the different modes of transportation, we do not believe using the memorandum of agreement between TSA and FAA as a framework is sufficient. The lack of clearly defined roles and responsibilities can lead to duplication, confusion, conflicts, and most importantly, gaps in preparedness.

   Although designating a DOT liaison to TSA is a step in the right direction, the roles and responsibilities of each entity and the coordinating processes need to be documented. Departures of key individuals within each entity, such as the designated DOT liaison to TSA, have the potential to erode informal networks. Given the importance of security efforts, coordinating processes between TSA and DOT need to be documented so that they span the terms of various administrations and individuals.

4. We agree that the Aviation and Transportation Security Act[1] (ATSA) gave TSA primary responsibility for securing all modes of transportation. However, neither this act, nor other legislation, has defined TSA roles and responsibilities in securing all modes of transportation. Specifically, ATSA does not specify TSA's roles and responsibilities in securing the maritime and land transportation modes

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

in detail as it does for aviation security. The act also did not eliminate DOT modal administrations' existing statutory responsibilities for securing the different modes of transportation. Moreover, recent legislation clarifies that DOT still has transportation 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 and define DOT's and TSA's roles and responsibilities in transportation security, we believe that these entities should establish a mechanism, such as a memorandum of agreement. Using such a mechanism would serve to clarify, delineate, and document the roles and responsibilities of each entity. It would also serve to hold each entity accountable for its transportation security responsibilities. Finally, it could serve as a vehicle to communicate the roles and responsibilities of each entity to transportation security stakeholders.

The mechanism—whether it is a memorandum of agreement or other document—used to clarify and define DOT's and TSA's roles and responsibilities should not be static. Rather, it should be a living document that changes as each entity's roles and responsibilities in transportation security matters evolve and events occur.

5. We disagree that all of DOT's ongoing security efforts are nonpolicy making activities. For example, the Research and Special Programs Administration issued regulations in March 2003 that requires shippers and carriers of hazardous materials to develop and implement security plans and to include a security component in their employee training programs.

   While DOT's role in security efforts may decrease in the future, it seems unlikely that DOT will be devoid of any security responsibilities in the future. For example, as noted in the report, 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. In addition, the Maritime Transportation Security Act of 2002[2] authorizes the Secretary of Transportation to train and certify maritime security professionals and establish a grant

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

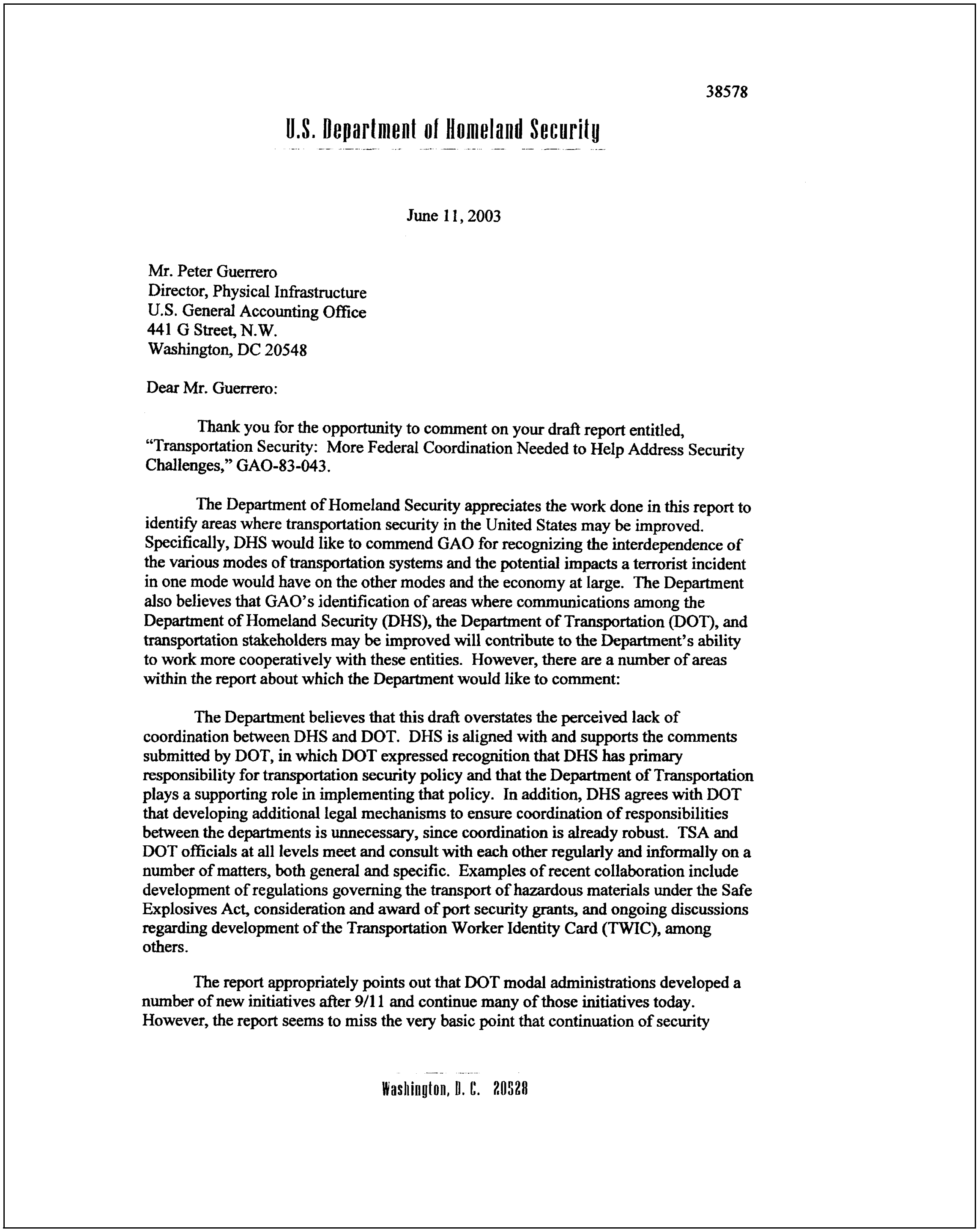
program to fund the implementation of Area Maritime Transportation Security Plans and facility security plans. Further, although the primary responsibility for securing the aviation system was transferred to TSA, FAA remains responsible for protecting the nation's air traffic control system—both the physical security of its air traffic control facilities and computer systems.

Although DOT recognizes that DHS has the lead in transportation security matters, it could be difficult to distinguish its role in maintaining transportation operations and improving transportation service and safety from DHS' role in securing the transportation system. Security is often intertwined with transportation operations and safety. For example, installing a fence around truck yards could be considered both a safety and security measure. Further security measures that restrict the flow of passengers or freight through the transportation system could have serious consequences on transportation operations. Because of these interactions and overlap, the roles and responsibilities of DOT and DHS in transportation safety and security can be blurred. Consequently, we continue to believe the entities should establish a mechanism to help clarify and delineate their roles and responsibilities in security matters.

Appendix III

Comments from the Department of Homeland Security

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



38578

U.S. Department of Homeland Security

June 11, 2003

Mr. Peter Guerrero
Director, Physical Infrastructure
U.S. General Accounting Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Guerrero:

Thank you for the opportunity to comment on your draft report entitled, "Transportation Security: More Federal Coordination Needed to Help Address Security Challenges," GAO-83-043.

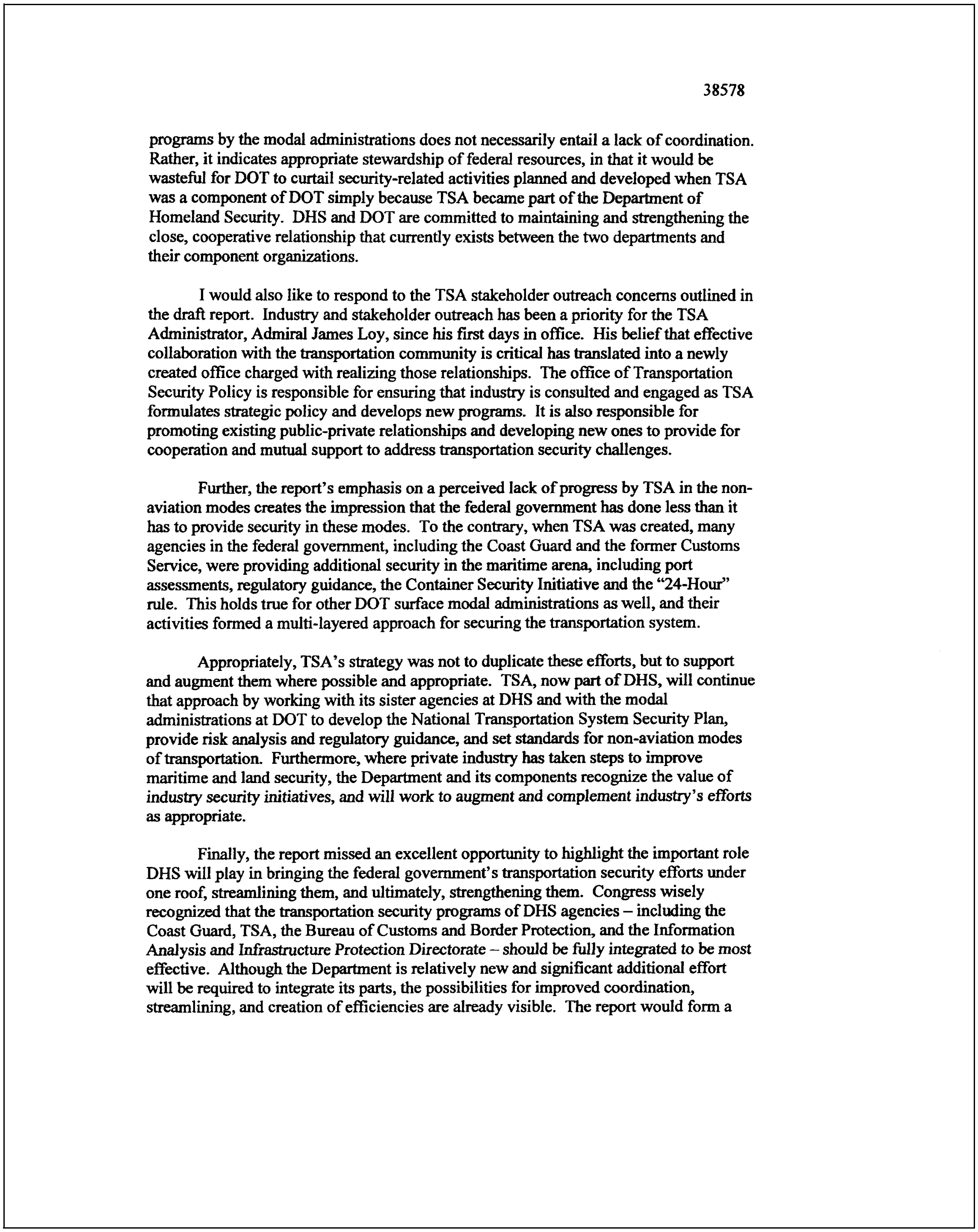
The Department of Homeland Security appreciates the work done in this report to identify areas where transportation security in the United States may be improved. Specifically, DHS would like to commend GAO for recognizing the interdependence of the various modes of transportation systems and the potential impacts a terrorist incident in one mode would have on the other modes and the economy at large. The Department also believes that GAO's identification of areas where communications among the Department of Homeland Security (DHS), the Department of Transportation (DOT), and transportation stakeholders may be improved will contribute to the Department's ability to work more cooperatively with these entities. However, there are a number of areas within the report about which the Department would like to comment:

See comment 1.

The Department believes that this draft overstates the perceived lack of coordination between DHS and DOT. DHS is aligned with and supports the comments submitted by DOT, in which DOT expressed recognition that DHS has primary responsibility for transportation security policy and that the Department of Transportation plays a supporting role in implementing that policy. In addition, DHS agrees with DOT that developing additional legal mechanisms to ensure coordination of responsibilities between the departments is unnecessary, since coordination is already robust. TSA and DOT officials at all levels meet and consult with each other regularly and informally on a number of matters, both general and specific. Examples of recent collaboration include development of regulations governing the transport of hazardous materials under the Safe Explosives Act, consideration and award of port security grants, and ongoing discussions regarding development of the Transportation Worker Identity Card (TWIC), among others.

The report appropriately points out that DOT modal administrations developed a number of new initiatives after 9/11 and continue many of those initiatives today. However, the report seems to miss the very basic point that continuation of security

Washington, D. C. 20528



38578

See comment 2.

programs by the modal administrations does not necessarily entail a lack of coordination. Rather, it indicates appropriate stewardship of federal resources, in that it would be wasteful for DOT to curtail security-related activities planned and developed when TSA was a component of DOT simply because TSA became part of the Department of Homeland Security. DHS and DOT are committed to maintaining and strengthening the close, cooperative relationship that currently exists between the two departments and their component organizations.

I would also like to respond to the TSA stakeholder outreach concerns outlined in the draft report. Industry and stakeholder outreach has been a priority for the TSA Administrator, Admiral James Loy, since his first days in office. His belief that effective collaboration with the transportation community is critical has translated into a newly created office charged with realizing those relationships. The office of Transportation Security Policy is responsible for ensuring that industry is consulted and engaged as TSA formulates strategic policy and develops new programs. It is also responsible for promoting existing public-private relationships and developing new ones to provide for cooperation and mutual support to address transportation security challenges.

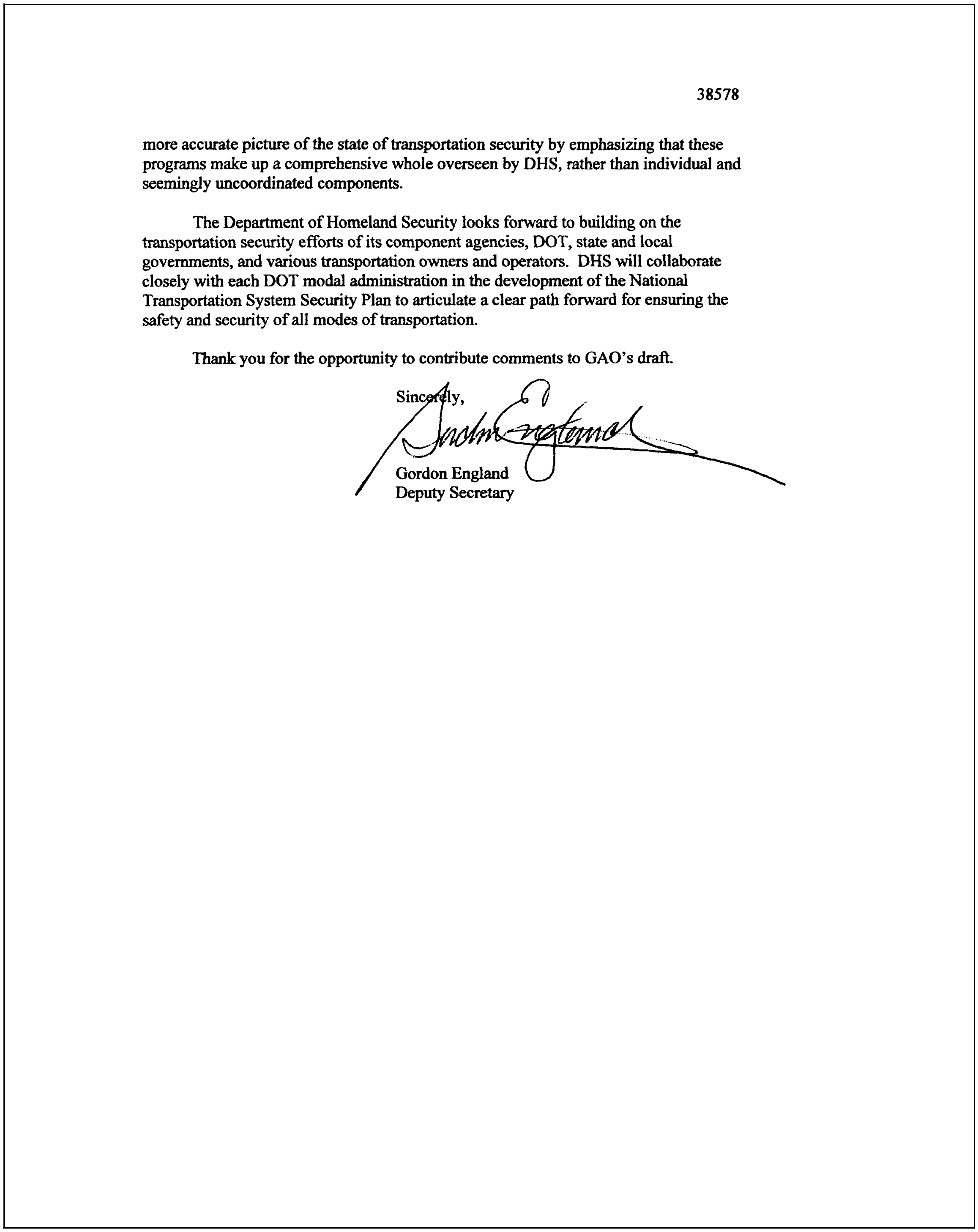
See comment 3.

Further, the report's emphasis on a perceived lack of progress by TSA in the non-aviation modes creates the impression that the federal government has done less than it has to provide security in these modes. To the contrary, when TSA was created, many agencies in the federal government, including the Coast Guard and the former Customs Service, were providing additional security in the maritime arena, including port assessments, regulatory guidance, the Container Security Initiative and the "24-Hour" rule. This holds true for other DOT surface modal administrations as well, and their activities formed a multi-layered approach for securing the transportation system.

Appropriately, TSA's strategy was not to duplicate these efforts, but to support and augment them where possible and appropriate. TSA, now part of DHS, will continue that approach by working with its sister agencies at DHS and with the modal administrations at DOT to develop the National Transportation System Security Plan, provide risk analysis and regulatory guidance, and set standards for non-aviation modes of transportation. Furthermore, where private industry has taken steps to improve maritime and land security, the Department and its components recognize the value of industry security initiatives, and will work to augment and complement industry's efforts as appropriate.

See comment 4.

Finally, the report missed an excellent opportunity to highlight the important role DHS will play in bringing the federal government's transportation security efforts under one roof, streamlining them, and ultimately, strengthening them. Congress wisely recognized that the transportation security programs of DHS agencies – including the Coast Guard, TSA, the Bureau of Customs and Border Protection, and the Information Analysis and Infrastructure Protection Directorate – should be fully integrated to be most effective. Although the Department is relatively new and significant additional effort will be required to integrate its parts, the possibilities for improved coordination, streamlining, and creation of efficiencies are already visible. The report would form a



38578

more accurate picture of the state of transportation security by emphasizing that these programs make up a comprehensive whole overseen by DHS, rather than individual and seemingly uncoordinated components.

The Department of Homeland Security looks forward to building on the transportation security efforts of its component agencies, DOT, state and local governments, and various transportation owners and operators. DHS will collaborate closely with each DOT modal administration in the development of the National Transportation System Security Plan to articulate a clear path forward for ensuring the safety and security of all modes of transportation.

Thank you for the opportunity to contribute comments to GAO's draft.

Sincerely,

Gordon England
Deputy Secretary

The following are GAO's comments on the Department of Homeland Security letter dated June 11, 2003.

GAO Comments

1. We disagree that the report overstates the lack of coordination between DHS and DOT and that mechanisms to ensure coordination of responsibilities is unnecessary. Although DHS and DOT report that they are coordinating on security matters, based on our discussions with representatives from state and local government and industry associations, it appears that there is a need to improve such efforts. As we noted throughout the report, representatives from several associations told us that they have received conflicting messages from the federal agencies involved in transportation security. Representatives from several associations also 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. Moreover, there appears to be a break down in communication between TSA and DOT about current security initiatives. For example, although TSA officials stated that they have informed DOT about their plans to issue security standards, some DOT officials we met with were unsure as to whether TSA was issuing standards, what the standards would entail, or the time frames for issuing the standards.

   We agree that the Aviation and Transportation Security Act[1] (ATSA) gave TSA primary responsibility for securing all modes of transportation. However, neither this act, or other legislation, has defined TSA's roles and responsibilities in securing all modes of transportation. Specifically, 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. The act also did not eliminate DOT modal administrations' existing statutory responsibilities for securing the different modes of transportation. Moreover, recent legislation clarifies that DOT still has transportation 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.

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

To clarify and define DOT's and TSA's roles and responsibilities in transportation security, we believe that these entities should establish a mechanism, such as a memorandum of agreement. Using such a mechanism would serve to clarify, delineate, and document the roles and responsibilities of each entity. It would also serve to hold each entity accountable for its transportation security responsibilities. Finally, it could serve as a vehicle to communicate the roles and responsibilities of each entity to transportation security stakeholders.

The mechanism—whether it is a memorandum of agreement or other document—used to clarify and define DOT's and TSA's roles and responsibilities should not be static. Rather, it should be a living document that changes as each entity's roles and responsibilities in transportation security matters evolve and events occur.

2. We disagree that the report suggests that the continuation of security efforts by the DOT modal administrations represents a lack of coordination. The report credits TSA for meeting a number of aviation security deadlines during its first year of existence and highlights the efforts of DOT modal administrations and other federal agencies to improve the security of all modes since September 11. We also note that TSA is beginning to assert a greater role in securing all modes of transportation and DOT modal administrations are continuing or launching new security efforts. We did not suggest that the continuation of such efforts by DOT modal administrations represents a lack of coordination. Rather, we noted that as both entities move forward with security efforts, it is increasingly important that the roles of TSA and DOT modal administrations are clearly defined. The lack of clearly defined roles and responsibilities can lead to duplication, confusion, conflicts, and most importantly, gaps in preparedness.

3. Our intention is not to suggest that the federal government's efforts to secure the non-aviation modes of transportation have been insufficient. To the contrary, we highlight the efforts by DOT modal administrations and other federal agencies to secure the maritime and land modes of transportation. We also recognize that TSA's aviation security focus during its first year of existence was primarily due to the ATSA deadlines.

4. We agree that the newly created DHS brings a number of agencies responsible for transportation security under one roof, which could ultimately improve coordination and streamline and strengthen

security efforts. However, this does not solve all the potential coordination problems we highlight in the report because important transportation stakeholders—specifically, the DOT modal administrations—are housed in another department. Because both DHS agencies and DOT modal administrations are moving forward with transportation security initiatives, it is critical that the roles and responsibilities of each entity are clearly delineated and communicated to all stakeholders and that they coordinate their security efforts. The lack of such clarification, communication, and coordination could create problems, such as duplication of efforts and gaps in preparedness.

Highlights of Current Laws and Regulations Governing Transportation Security

Table 5: Authorizations

Public law - Authorization	Modes impacted	Key provisions	Related target dates for compliance
Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 597 et seq. (2001). November 19, 2001	All	Established Transportation Security Administration (TSA), responsible for, *inter alia*, security in all modes of transportation.	11/19/2001
	Aviation	Established a more comprehensive federal air marshals program for international and domestic flights.	
	Aviation	Deployment of federal law enforcement officers at airports to meet aviation safety and security concerns.	
	Aviation	Directed FAA, in consultation with TSA, to develop security-training programs for flight and cabin crew.	1/18/02
	Aviation	Deployment of federal personnel for the screening of passengers and baggage at airports.	11/19/02
	Aviation	Appointed Federal Security Managers to oversee the screening of passengers and baggage at each airport.	11/19/02
	Aviation	Authorizes TSA to deploy explosive detection systems (EDS) or equivalent measures allowed by law at all U.S. airports.	12/31/2002
	Aviation	Authorized $500,000,000 (FY 2002) for FAA to provide federal grants to fortify cockpit doors and for other aircraft security measures.	4/1/2003

(Continued From Previous Page)

Public law - Authorization	Modes impacted	Key provisions	Related target dates for compliance
Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 et seq. (2002). November 25, 2002	All	Creates the Department of Homeland Security.	
	All	Creates Border and Transportation Security Directorate, responsible for maintaining the security of borders and transportation systems.	
	Aviation	Training and deputizing pilots to be Federal Flight Deck Officers to defend the flight decks of aircrafts in flight.	2/25/2003
	All	Transferred Transportation Security Administration and Coast Guard from Department of Transportation to Department of Homeland Security.	3/1/2003
	Aviation	Moved date for EDS installation in all U.S. airports.	12/31/2003
	All	Requires all companies that transport or ship explosives to give the ATF the names and identifying information of all employees authorized to possess explosive materials. Requires the ATF to conduct background checks of employees to determine if they are prohibited from possessing explosive materials.	
	All	Expands the responsibilities of the Research and Special Programs Administration (RSPA), within the Department of Transportation, for regulating hazardous materials to include hazardous materials transportation security.	
	All	Protects critical infrastructure information voluntarily submitted to a covered federal agency from the Freedom of Information Act and other federal and state disclosure requirements.	

(Continued From Previous Page)

Public law - Authorization	Modes impacted	Key provisions	Related target dates for compliance
Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, 116 Stat. 2064 (2002). November 25, 2002	Seaport	Set up a National Maritime Transportation Security Plan.	
		Implement Area Maritime Transportation Security Plans and coordinate area plans.	
		Develop and maintain an antiterrorism cargo identification, tracking, and screening system for containerized cargo.	
		To assign Coast Guard personnel as sea marshals to deter or respond to acts of terrorism.	
		Authorizes the Secretary of Transportation to train and certify maritime security professionals.	
		Establishes a program to evaluate and certify systems of international intermodal transportation.	
		The Coast Guard shall conduct a vulnerability assessment of facilities and vessels that may be involved in a transportation security incident at least every 5 years.	
		The Secretary of Homeland Security shall issue biometric transportation security cards and enhanced crew-member identification for individuals who require access to secure areas of vessels and port facilities.	
		The Secretary of Transportation, acting through the Maritime Administration, shall establish a grant program to fund the implementation of Area Maritime Transportation Security Plans and facility security plans.	
USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). October 26, 2001	All	Mandates federal background checks of individuals operating vehicles carrying hazardous materials.	
		Criminalizes terrorist attacks and other acts of violence against mass transportation systems.	10/26/2001
Pipeline Safety Improvement Act of 2002, Pub. L. No. 107-355, 116 Stat. 2985 (2002). December 17, 2002	Pipeline	Authorizes the Secretary of Transportation to reinforce pipeline facilities deemed potentially unsafe or vulnerable to terrorist attacks.	
Trade Act of 2002, Pub. L. No. 107-210, 116 Stat. 933 (2002). August 6, 2002	All	Authorizes the Secretary of Commerce to create an electronic data interchange system to ensure transportation safety and security of cargo.	

Source: GAO analysis of U.S. Code.

Table 6: Appropriations

Public law – appropriation	Modes impacted	Key provisions	Funding appropriated
2001 Emergency Supplemental Appropriations Act for Recovery from and Response to Terrorist Attacks on the United States, Pub. L. No. 107-38, 115 Stat. 220 (2001). September 18, 2001	All	Provided funding for increased transportation security. Provided funding for repairing public facilities and transportation systems damaged by the attacks.	Specific appropriations are found in the Pub. L. No. 107-117.
2002 Department of Transportation Appropriations Act, Pub. L. No. 107-87, 115 Stat. 833 (2001). December 18, 2001	Aviation	Provided funding for TSA for civil aviation security services pursuant to the Aviation and Transportation Security Act.	$1,250,000,000 (app. FY 2002)
	Aviation	Provided funding for FAA operations for civil aviation security program activities.	$150,154,000 (app. FY 2002)
Department Of Defense And Emergency Supplemental Appropriations for Recovery From and Response to Terrorist Attacks on the United States Act, 2002, Pub. L. No. 107-117, 115 Stat. 2230 (2002). January 10, 2002	Seaport	Funding for a port security program.	$93,300,000 (app. FY 2002)
	Seaport	Funding for Coast Guard for their response to 9/11 terrorist attacks.	$209,150,000 (app. FY 2002)
	Aviation	Funding for FAA for their response to 9/11 terrorist attacks.	$535,500,000 (app. FY 2002)
	Highway	Funding for Federal Highway Administration for their response to 9/11 terrorist attacks.	$175,000,000 (app. FY 2002)
	Transit	Funding for Federal Transit Administration for their response to 9/11 terrorist attacks.	$123,000,000 (app. FY 2002)
	Rail	Funding for Federal Railroad Administration for their response to 9/11 terrorist attacks.	$106,000,000 (app. FY 2002)
	All	Funding for Research and Special Programs Administration.	$2,500,000 (app. FY 2002)

(Continued From Previous Page)

Public law – appropriation	Modes impacted	Key provisions	Funding appropriated
2002 Supplemental Appropriations Act for Further Recovery from and Response to Terrorist Attacks on the United States, Pub. L. No. 107-206, 116 Stat. 820 (2002). August 2, 2002	Aviation	Provides for the installation of explosives detection systems in commercial service airports.	$738,000,000 (app. FY 2003)
	Seaport	Provides funds for port security activities, including Port Security Grants.	$125,000,000 (app. FY 2003)
	Seaport	Appropriates funds for the port security pilot program, Operation Safe Commerce.	$28,000,000 (app. FY 2003)
	Motor Coach	Appropriates grants and contracts to enhance security for intercity bus operations.	$15,000,000 (app. FY 2003)
	Aviation	Funds for procurement of air-ground communications systems and devices for the Federal Air Marshal Program.	$15,000,000 (app. FY 2003)
	All	Funds for grants and contracts for radiation detection system test and evaluation.	$4,000,000 (app. FY 2003)
	Aviation	Funds for grants to airport authorities for pilot projects to improve airport terminal security.	$17,000,000 (app. FY 2003)
	All	Funds for grants and contracts for security, research, development and pilot projects.	$10,000,000 (app. FY 2003)
	Aviation	Funds for replacement of magnetometers at airport passenger screening locations in commercial service airports.	$23,000,000 (app. FY 2003)

(Continued From Previous Page)

Public law – appropriation	Modes impacted	Key provisions	Funding appropriated
Consolidated Appropriation Resolution for 2003, Pub. L. No. 108-7, 117 Stat. 11 (2003). February 20, 2003	Aviation	Provides for aviation security (screening activities, airport support, and enforcement presence) including:	$4,516,300,000 (app. FY 2003) including:
		additional funding from FAA appropriations for explosives detections systems	$144,000,000 (app. FY 2003)
		additional funding for terminal modifications needed for the installation of EDS equipment	$265,000,000 (app. FY 2003)
		additional funding for the procurement of checked baggage EDS equipment	$174, 500,000 (app. FY 2003)
	All	Funds administrative, including intelligence, activities of the Transportation Security Administration.	$308,700,000 (app. FY 2003)
	All	Enhances maritime and land security including:	$244,800,000 (app. FY 2003) including:
		provides additional funding for port security grants	$150,000,000 (app. FY 2003)
		funds for radiation detection and monitoring system evaluation and procurement	$4,000,000 (app. FY 2003)
		funds for the purpose of deploying Operation Safe Commerce	$30,000,000 (app. FY 2003)
	All	Appropriates funds for research and development related to transportation security including:	$110, 200,000 (app. FY 2003) including:
		funds for grants for port security	$10,000,000 (app. FY 2003)
Emergency Wartime Supplemental Appropriations Act for FY 2003, Pub. L. No. 108-11, 117 Stat. 559 (2003)	Aviation	Provides financial assistance to US flag air carriers for expenses and revenue forgone related to aviation security.	$2,395,750,000 of which the first $100 million is to reimburse carriers for strengthening cockpit doors. (app. FY 2003)
	Seaport	Appropriates funds for the Coast Guard to support Operation Liberty Shield.	$228,000,000 (app. FY 2003)
	Aviation	Appropriates additional funds to TSA for the installation of explosive detection systems at airports.	$235,000,000 (app. FY 2003)
	Seaport	Appropriates additional funds to TSA for port security.	$20,000,000 (app. FY 2003)
	Aviation	Appropriates additional funds to TSA for passenger screener hiring, training, and related costs.	$280,000,000 (app. FY 2003)

Source: GAO analysis of U.S. Code.

Table 7: Regulations

Regulations[a]	Modes impacted	Issuing agency	Key provisions
Criminal History Records Checks, 66 Fed. Reg. 63474 (Dec. 6, 2001). Effective December 6, 2001	Aviation	FAA	Requires airport operators and aircraft operators to conduct fingerprint-based criminal history records checks (CHRC's) of individuals with unescorted access authority to secured areas.
Civil Aviation Security Rules, 67 Fed. Reg. 8340 (Feb. 22, 2002). Effective February 17, 2002	All	TSA	Transfers rules governing civil aviation security to TSA.
			Provides screener qualifications and training.
			Defines and governs the release of "sensitive security information."
Security Programs for Aircraft 12,500 Pounds or More, 67 Fed. Reg. 8205 (Feb. 22, 2002). Effective June 24, 2002	Aviation	TSA	Requires aircraft operators of aircraft with a maximum takeoff weight of 12,500 lbs. or more to conduct criminal history records checks on flightcrew members.
			Requires access to the flight deck of such aircraft be restricted.
Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States, 67 Fed. Reg. 42710 (June 25, 2002). Effective June 25, 2002	Aviation	Customs Service	Requires air carriers, upon request, to electronically provide U.S. Customs Service with access to Passenger Name Record (PNR) information concerning the identity and travel plans of passengers for any international flight to or from the United States.
Picture Identification Requirements, 67 Fed. Reg. 65858 (Oct. 28, 2002). Effective October 28, 2002	Aviation	FAA	Requires all certified pilots to carry photo identification subject to inspection upon request from the FAA or any federal, state, or local law enforcement officer.
Discretionary Bridge Candidate Rating Factor, 67 Fed. Reg. 63539 (Oct. 15, 2002). Effective November 14, 2002	Highways	Federal Highway Administration	Allows discretionary bridge funds to be used for security improvements on eligible bridges, subject to 23 USC 144 requirements.
Presentation of Vessel Cargo Declaration to Customs Before Cargo Is Laden Aboard Vessel at Foreign Port for Transport to the United States, 67 Fed. Reg. 66318 (Oct. 31, 2002). Effective December 2, 2002.	Seaport	Customs Service	Requires the advance and accurate presentation of certain manifest information prior to lading at the foreign port, in order to enable Customs to evaluate the risk of smuggling weapons of mass destruction.
Aviation Security: Private Charter Security Rules, 67 Fed. Reg. 79881 (Dec. 31, 2002). Effective February 1, 2003	Aviation	TSA	Requires private charter operators using aircraft with a maximum takeoff weight of at least 100,000 lbs. or which can seat at least 61 passengers to ensure that passengers and their carry-on baggage are screened prior to boarding.

(Continued From Previous Page)

Regulations[a]	Modes impacted	Issuing agency	Key provisions
Coast Guard Transition to Department of Homeland Security, 68 Fed. Reg. 9533 (Feb. 28, 2003). Effective March 1, 2003	Seaport	Coast Guard	Transfers the Coast Guard from the Department of Transportation to the newly created Department of Homeland Security.
Organization and Delegation of Powers and Duties, Update of Secretarial Delegations, 68 Fed. Reg. 10988 (March 7, 2003). Effective March 7, 2003	Motor Carrier	Office of the Secretary, DOT	Transfers authority of the Federal Motor Carrier Safety Administration to determine security risks to the Transportation Security Administration.
Screening of Aliens and Other Designated Individuals Seeking Flight Training, 68 Fed. Reg. 7313 (Feb. 13, 2003). Effective March 17, 2003	Aviation	DOJ	Prohibits aviation training providers to train aliens or other designated individuals without prior approval by the Attorney General.
Security Requirements for Motor Carriers Transporting Hazardous Materials, 68 Fed. Reg. 13250 (March 19, 2003). Effective March 19, 2003	Motor Carrier	Federal Motor Carrier Safety Administration (FMCSA)	Transfers rulemaking authority addressing the security of motor carrier shipments of hazardous materials to the Research and Special Programs Administration (RSPA) from the FMCSA.
Hazardous Materials: Security Requirements for Offerors and Transporters of Hazardous Materials, 68 Fed. Reg. 14510 (March 25, 2003). Effective March 25, 2003	All	RSPA	Requires shippers and carriers of certain highly hazardous materials to develop and implement security plans.
			Requires all shippers and carriers of hazardous materials to include a security component in their employee training programs.
Notification of Arrival in U.S. Ports, 68 Fed. Reg. 9537 (Feb. 28, 2003) Effective April 1, 2003.	Seaport	Coast Guard	Makes permanent changes in notification of arrival and departure requirements to ensure public safety and security, including requiring electronic submission of cargo manifest information to the U.S. Customs Service, and requiring additional crew and passenger information.
Organization and Delegation of Powers and Duties; Delegation to the Administrator, Maritime Administrator, 68 Fed. Reg. 16215 (April 3, 2003). Effective April 3, 2003	Seaport	Office of the Secretary, DOT	Transfers authority to the Maritime Administrator to develop standards and curriculum for the training and certification of maritime security professionals.

(Continued From Previous Page)

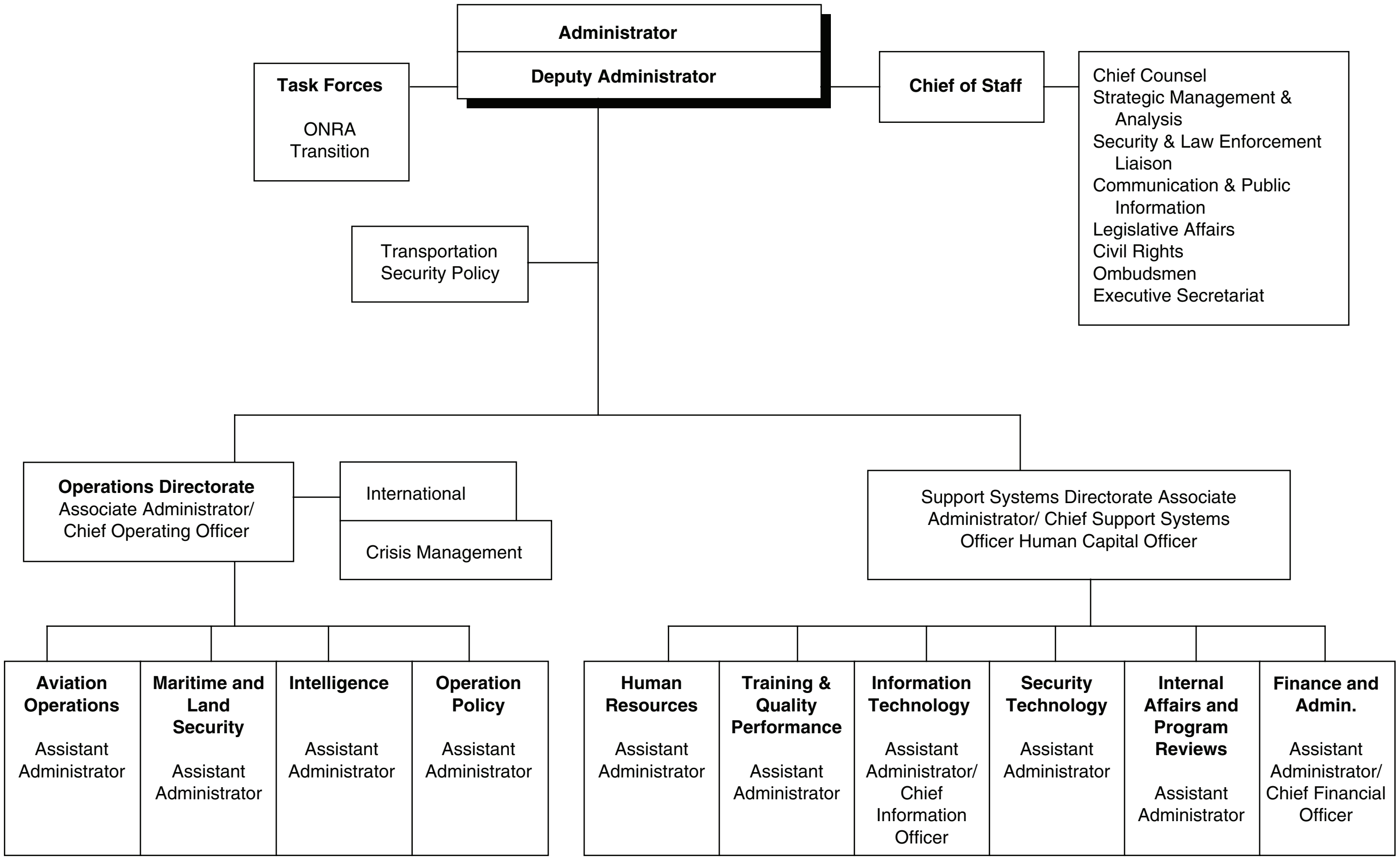
Regulations[a]	Modes impacted	Issuing agency	Key provisions
Implementation of the Safe Explosives Act, 68 Fed. Reg. 13768 (March 20, 2003). Effective May 24, 2003 **Interim Final Rule**	All	ATF	Requires applicants for licenses and permits to provide with the application the names and appropriate identifying information regarding employees authorized to possess explosive materials.
			Requires applicants for licenses and permits to provide with the application fingerprints and photographs of “responsible persons” (for example, site managers, sole proprietors, partners, corporate officers and directors, and majority shareholders).
			Requires the ATF to conduct background checks on responsible persons and employees authorized to possess explosive materials.
Limitations on the Issuance of Commercial Driver's Licenses with a Hazardous Materials Endorsement, 68 Fed. Reg. 23844 (May 5, 2003). Effective May 5, 2003 **Interim Final Rule**	Motor Carrier	FMCSA	Prohibits States from issuing, renewing, transferring, or upgrading a commercial driver’s license (CDL) with a hazardous material endorsement unless TSA has conducted a background check of the applicant, including administering a hazardous materials knowledge test.
Hazardous Materials: Enhancing Hazardous Materials Transportation Security 68 Fed. Reg. 23832 (May 5, 2003) Effective May 5, 2003 **Interim Final Rule**	Motor Carrier, Seaport	RSPA	Requires shippers and transporters to comply with Federal security regulations that apply to motor carrier and vessel transportation
			Requires applicants for exemptions from the Hazardous Materials Regulations compliance with applicable Federal transportation security laws and regulations.
Security Threat Assessment for Individuals Applying for a Hazardous Materials Endorsement for a Commercial Drivers License 68 Fed. Reg. 23852 (May 5, 2003) Effective May 5, 2003 **Interim Final Rule**	Motor Carrier	TSA	Establishes security threat assessment standards for determining whether an individual poses a security threat warranting denial of a hazardous materials endorsement for a CDL. Also established appeals and waiver procedures.

Source: GAO analysis of Code of Federal Regulations.

[a] All regulations listed are final rules unless otherwise noted.

Appendix V

Organizational Chart of the Transportation Security Administration



Source: TSA.

GAO Contacts and Staff Acknowledgments

GAO Contact

Cathleen Berrick, (202) 512-8777
Susan Fleming, (202) 512-4431
Peter Guerrero, (202) 512-2834

Acknowledgments

In addition to those named above, Steven Calvo, Nikki Clowers, Michelle Dresben, Glenn Dubin, Scott Farrow, Libby Halperin, David Hooper, Hiroshi Ishikawa, Ray Sendejas, and Glen Trochelman made key contributions to this report.

Related GAO Products

Transportation Security Reports and Testimonies

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

PRINTED ON ♲ RECYCLED PAPER

[redacted]