United States General Accounting Office

GAO

Testimony

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

For Release on Delivery
Expected at 10:00 a.m. EST
on Tuesday
March 23, 2004

RAIL SECURITY

Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain

Statement of Peter F. Guerrero, Director, Physical Infrastructure Issues; and Norman J. Rabkin, Managing Director, Homeland Security and Justice Issues

GAO
Accountability * Integrity * Reliability

G A O
Accountability•Integrity•Reliability

Highlights

Highlights of GAO-04-598T, a report to Committee on Commerce, Science, and Transportation, U.S. Senate

Why GAO Did This Study

Passenger and freight rail services are important links in the nation's transportation system. Terrorist attacks on passenger and/or freight rail services have the potential to cause widespread injury, loss of life, and economic disruption. The recent terrorist attack in Spain illustrates that rail systems, like all modes of transportation, are targets for attacks. GAO was asked to summarize the results of its recent reports on transportation security that examined (1) challenges in securing passenger and freight rail systems, (2) actions rail stakeholders have taken to enhance passenger and freight rail systems, and (3) future actions that could further enhance rail security.

What GAO Recommends

In our previous report on transportation security (GAO-03-843), we recommended that the Department of Homeland Security and Transportation use a mechanism, such as a memorandum of agreement, to clarify and delineate TSA's and DOT's roles and responsibilities in transportation security matters. DHS and DOT generally agreed with the report's findings; however, they disagreed with the recommendation. We continue to believe our recommendation has merit and would help address security challenges.

www.gao.gov/cgi-bin/getrpt?GAO-04-598T.

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.

March 23, 2004

RAIL SECURITY

Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain

What GAO Found

Securing the passenger and freight rail systems are fraught with challenges. Some of these challenges are common to passenger and freight rail systems, such as the funding of security improvements, the interconnectivity of the rail system, and the number of stakeholders involved in rail security. Other challenges are unique to the type of rail system. For example, the open access and high ridership of mass transit systems make them both vulnerable to attack and difficult to secure. Similarly, freight railroads transport millions of tons of hazardous materials each year across the United States, raising concerns about the vulnerability of these shipments to terrorist attack.

Passenger and freight rail stakeholders have taken a number of steps to improve the security of the nation's rail system since September 11, 2001. Although security received attention before September 11, the terrorist attacks elevated the importance and urgency of transportation security for passenger and rail providers. Consequently, passenger and freight rail providers have implemented new security measures or increased the frequency or intensity of existing activities, including performing risk assessments, conducting emergency drills, and developing security plans. The federal government has also acted to enhance rail security. For example, the Federal Transit Administration has provided grants for emergency drills and conducted security assessments at the largest transit agencies, among other things.

Implementation of risk management principles and improved coordination could help enhance rail security. Using risk management principles can help 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. In addition, improved coordination among federal entities could help enhance security efforts across all modes, including passenger and freight rail systems. We reported in June 2003 that the roles and responsibilities of the Transportation Security Administration (TSA) and the Department of Transportation (DOT) in transportation security, including rail security, have yet to be clearly delineated, which creates the potential for duplicating or conflicting efforts as both entities work to enhance security.

Mr. Chairman and Members of the Committee:

We appreciate the opportunity to provide testimony on the security of our nation's rail systems. Although most of the early attention following the September 11 attacks focused on aviation security, emphasis on the other modes of transportation has since grown as concerns are voiced about possible vulnerabilities, such as introducing weapons of mass destruction into this country through ports or launching chemical attacks on mass transit systems. Moreover, terrorist attacks around the world, such as the recent terrorist attack in Spain, have shown that rail systems, like all modes of transportation, are potential targets of attack.

As you requested, our testimony today focuses on (1) challenges in securing rail systems, (2) steps rail stakeholders have taken to enhance security since September 11, and (3) future actions that could further enhance rail security. Our comments are based on our reports and testimonies on the security of the entire transportation system, the security of mass transit systems, and railroad safety and security[1] as well as a body of our work undertaken since September 11 on homeland security and combating terrorism.

Summary

- Securing passenger and freight rail systems is fraught with challenges. Some security challenges are common to passenger and freight rail systems, such as the funding of security improvements, the interconnectivity of the rail system, and the number of stakeholders involved in rail security. For instance, government agencies at the federal, state, and local levels and private companies share responsibility for rail security. The number of stakeholders involved in transportation security can lead to

[1] U.S. General Accounting Office, *Transportation Security: Federal Action Needed to Help Address Security Challenges*, GAO-03-843 (Washington, D.C.: June 30, 2003); Rail *Safety and Security: Some Actions Already Taken to Enhance Rail Security, but Risk-based Plan Needed,* GAO-03-435 (Washington, D.C.: April 30, 2003); and *Mass Transit: Federal Action Could Help Transit Agencies Address Security Challenges,* GAO-03-263 (Washington, D.C.: December 13, 2002).

communication challenges, duplication, and confusion. Other security challenges are unique to the type of rail system. For example, the transport of hazardous materials by rail is of particular concern because serious incidents involving these materials have the potential to cause widespread disruption or injury. We recommended in April 2003 that DOT and DHS develop a plan that specifically addresses the security of the nation's freight rail infrastructure.[2] DHS has informed us that this plan is in progress.

- Passenger and freight rail providers have acted to enhance security since September 11. For example, passenger and freight rail providers have implemented new security measures or increased the frequency or intensity of existing activities, such as performing risk assessments, conducting emergency drills, and developing security plans. The federal government has also taken steps to try to enhance rail security. In the wake of September 11, Congress created the Transportation Security Administration (TSA) and gave it responsibility for the security of all modes of transportation. As TSA worked to establish itself and improve the security of the aviation system during its first year of existence, the Department of Transportation's (DOT) modal administrations acted to enhance passenger and freight rail security. For example, the Federal Transit Administration provided grants for emergency drills to mass transit agencies and the Federal Railroad Administration assisted commuter railroads with the development of security plans. 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, including rail security. We reported in June 2003 that TSA was moving forward with efforts to secure the entire transportation system, such as developing standardized criticality, threat, and vulnerability assessment tools, and establishing security standards for all modes of transportation.

- Although actions have been taken to enhance passenger and freight security since September 11, the recent terrorist attack on a rail system in Spain naturally focuses

[2] GAO-03-435.

our attention on what more could be done to secure the nation's rail systems. In our previous work on transportation security, we identified future actions that the federal government could take to enhance security of individual transportation modes as well as the entire transportation system. Two recurring themes cut across our previous work in transportation security—the need for the federal government to utilize a risk management approach and improve coordination of security efforts. Using risk management principles can help 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. A risk management approach can help inform funding decisions for security improvements within the rail system and across modes. We reported in June 2003 that TSA planned to adopt a risk management approach for its efforts to enhance the security of the nation's transportation system. In addition, improved coordination among rail stakeholders could help enhance security efforts across all modes, including passenger and freight rail systems. We reported in June 2003 that the roles and responsibilities of TSA and DOT in transportation security, including rail security, have yet to be clearly delineated, which creates the potential for duplicating or conflicting efforts as both entities work to enhance security. To clarify the roles and responsibilities of TSA and DOT in transportation security matters, we recommended that the Secretary of Transportation and the Secretary of Homeland Security use a mechanism, such as a memorandum of agreement, to clearly delineate their roles and responsibilities. To date, this recommendation has not been implemented.

Background

Passenger and freight rail services help move people and goods through the transportation system, which helps the economic well-being of the United States. Passenger rail services can take many forms. Some mass transit agencies, which can be public or private entities, provide rail services, such as commuter rail and heavy rail (e.g., subway) in cities across the United States.[3] Through these rail services, mass transit agencies serve a large part of the commuting population. For example, in the third quarter of 2003, commuter rail systems provided an average of 1.2 million passenger trips each weekday. The National Railroad Passenger Corporation (Amtrak) provides intercity passenger rail services in the United States. Amtrak operates a 22,000-mile network, primarily over freight railroad tracks, providing service to 46 states and the District of Columbia. In fiscal year 2002, Amtrak served 23.4 million passengers, or about 64,000 passengers per day. The nation's freight rail network carries 42 percent of domestic intercity freight (measured by ton miles) in 2001—everything from lumber to vegetables, coal to orange juice, grain to automobiles, and chemicals to scrap iron.

Prior to September 11, 2001, DOT—namely, the Federal Railroad Administration (FRA), Federal Transit Administration (FTA), and Research and Special Programs Administration (RSPA)—was the primary federal entity involved in passenger and freight rail 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.[4] The act also gives TSA regulatory authority over all transportation modes. With the passage of the Homeland Security Act, TSA, along with over 20 other agencies, was transferred to the new Department of Homeland Security (DHS).[5]

Throughout the world, rail systems have been the target of terrorist attacks. 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 about 5,500. In addition, according to the Mineta

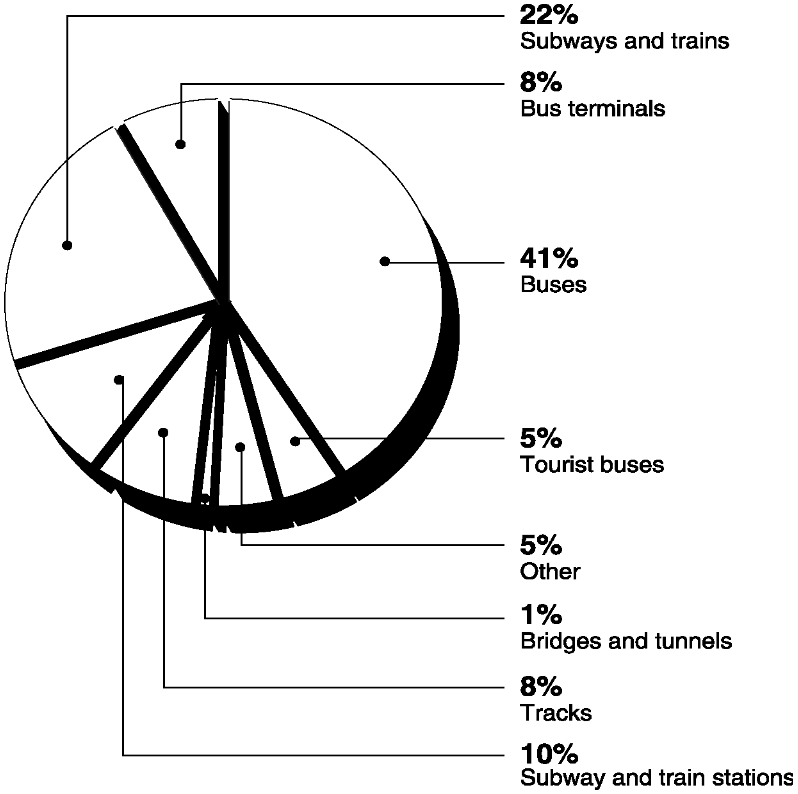
[3] Commuter rail is characterized by passenger trains operating on railroad tracks and providing regional service (e.g., between a central city and adjacent suburbs). Heavy rail is an electric railway that can carry a heavy volume of traffic. Heavy rail is characterized by high speed and rapid acceleration, passenger rail cars operating singly or in multicar trains on fixed rails, separate rights-of-way from which all other vehicular and foot traffic is excluded, sophisticated signaling, and high-platform loading. Most subway systems are considered heavy rail.

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

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

Institute,[6] surface transportation systems were the target of more than 195 terrorist attacks from 1997 through 2000. (See fig. 1.)

Figure 1: Targets of Attacks on Public Surface Transportation Systems Worldwide, 1997 to 2000



Source: Based on information from the Mineta Transportation Institute.

Numerous Challenges Exist in Securing Rail Systems

Passenger and freight rail providers face significant challenges in improving security. Some security challenges are common to passenger and freight rail systems; others are unique to the type of rail system. Common challenges include the funding of security improvements, the interconnectivity of the rail system, and the number of stakeholders

[6] The Mineta Transportation Institute was established by Congress as part of the Intermodal Surface Transportation Efficiency Act of 1991 (ISTEA). The Mineta Institute focuses on international surface transportation policy issues

involved in rail security. The unique challenges include the openness of mass transit systems and the transport of hazardous materials by freight railroads.

Common Security Challenges Confront Passenger and Freight Rail Systems

A challenge that is common to both passenger and freight rail systems is the funding of security enhancements. Although some security improvements are inexpensive, such as removing trash cans from subway platforms, most require substantial funding. For example, as we reported in December 2002, one transit agency estimated that an intrusion alarm and closed circuit television system for only one of its portals would cost approximately $250,000—an amount equal to at least a quarter of the capital budgets of a majority of the transit agencies we surveyed.[7] The current economic environment makes this a difficult time for private industry or state and local governments to make additional security investments. As we noted in June 2003, the sluggish economy has further weakened the transportation industry's financial condition by decreasing ridership and revenues. Given the tight budget environment, state and local governments and transportation operators, such as transit agencies, must make difficult trade-offs between security investments and other needs, such as service expansion and equipment upgrades. Further exacerbating the problem of funding security improvements are the additional costs the passenger and freight rail providers incur when the federal government elevates the national threat condition. For example, Amtrak estimates that it spends an additional $500,000 per month for police overtime when the national threat condition is increased.

Another common challenge for both passenger and freight rail systems is the interconnectivity within the rail system and between the transportation sector and nearly every other sector of the economy. The passenger and freight rail systems are part of an intermodal transportation system—that is, 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

as related to three primary responsibilities: research, education, and technology transfer.

train to truck. The interconnective nature of the transportation system creates several security challenges. First, the effects of events directed at one mode of transportation can ripple throughout the entire system. For example, when the port workers in California, Oregon, and Washington went on strike in 2002, the railroads saw their intermodal traffic decline by almost 30 percent during the first week of the strike, compared with the year before. Second, the interconnecting modes can contaminate each other—that is, if a particular mode experiences a security breach, the breach could affect other modes. 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 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 by the security efforts, or lack thereof, in the other modes. Third, intermodal facilities where passenger and freight rail systems connect and interact with other transportation modes—such as ports—are potential targets for attack because of the presence of passengers, freight, employees, and equipment at these facilities.

An additional common challenge for both passenger and rail systems is the number of stakeholders involved. Government agencies at the federal, state, and local levels and private companies share responsibility for rail security. For example, there were over 550 freight railroads operating in the United States in 2002. In addition, many passenger rail services, such as Amtrak and commuter rail, operate over tracks owned by freight railroads. For instance, over 95 percent of Amtrak's 22,000-mile network operates on freight railroad tracks.[8] The number of stakeholders involved in transportation security can lead to communication challenges, duplication, and conflicting guidance. As we have noted in past reports, coordination and consensus-building are critical to successful implementation of security efforts.[9] Transportation stakeholders can have inconsistent

[7] GAO-03-263.

[8] Freight railroads and commuter rail agencies also operate between Boston Massachusetts, and Washington, D.C., on the Northeast Corridor, which is primarily owned by Amtrak.

[9] U.S. General Accounting Office, *Mass Transit: Challenges in Securing Transit Systems*, GAO-02-1075T (Washington, D.C.: Sept. 18, 2002); U.S. General Accounting Office, *Homeland Security: Effective Intergovernmental Coordination Is Key to Success*, GAO-02-1011T (Washington, D.C.: Aug. 20, 2002); and, U.S. General Accounting Office, *National Preparedness: Integration of Federal, State, Local, and Private*

goals or interests, which can make consensus-building challenging. For example, from a safety perspective, trains that carry hazardous materials should be required to have placards that identify the contents of a train 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.

Passenger and Freight Rail Systems Also Face Unique Challenges

In addition to the common security challenges that face both passenger and rail systems, there are some challenges that are unique to the type of rail system. In our past reports, we have discussed several of these unique challenges, including the openness of mass transit systems and the size of the freight rail network and the diversity of freight hauled.

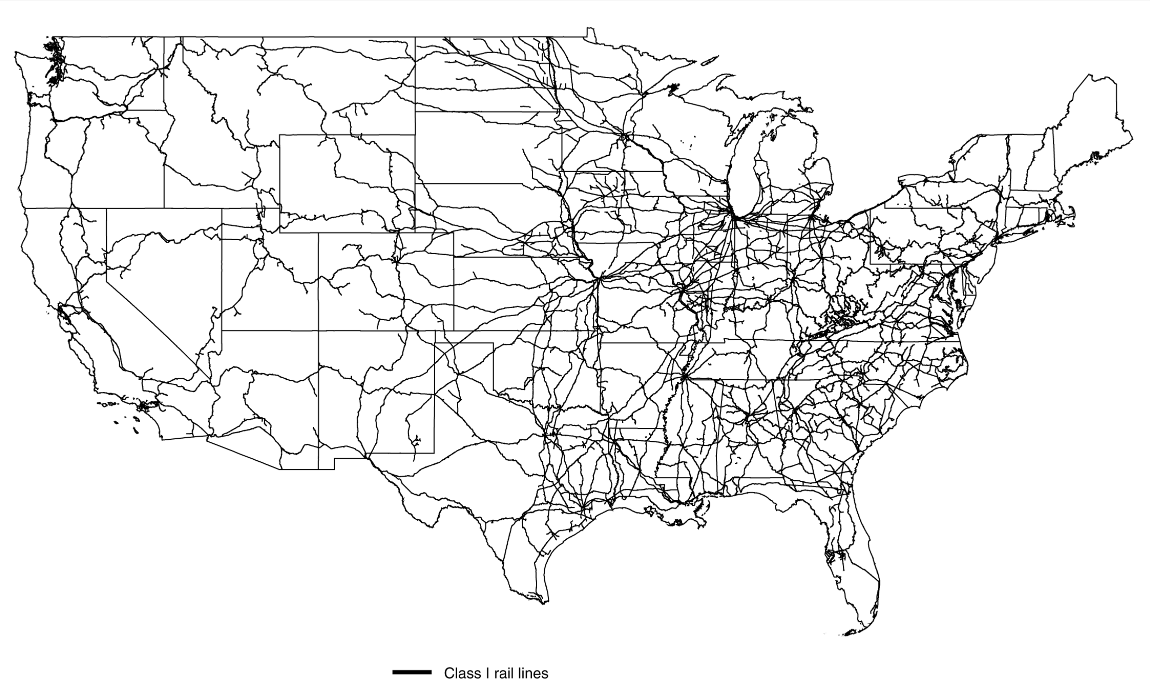
According to mass transit officials and transit security experts, certain characteristics of mass transit systems make them inherently vulnerable to terrorist attacks and difficult to secure. By design, mass transit systems are open (i.e., have multiple access points and, in some cases, no barriers) so that they can move large numbers of people quickly. In contrast, the aviation system is housed in closed and controlled locations with few entry points. The openness of mass transit systems can leave them vulnerable because transit officials cannot monitor or control who enters or leaves the systems. In addition, other characteristics of some transit systems—high ridership, expensive infrastructure, economic importance, and location (e.g., large metropolitan areas or tourist destinations)—also make them attractive targets because of the potential for mass casualties and economic damage. Moreover, some of these same characteristics make mass transit systems difficult to secure. For example, the number of riders that pass through a mass transit system—especially during peak hours—make some security measures, such as metal detectors, impractical. In addition, the multiple access points along extended routes make the costs of securing each location prohibitive.

Sector Efforts Is Critical to an Effective National Strategy for Homeland Security, GAO-02-621T (Washington, D.C.: Apr. 11, 2002).

Further complicating transit security is the need for transit agencies to balance security concerns with accessibility, convenience, and affordability. Because transit riders often could choose another means of transportation, such as a personal automobile, transit agencies must compete for riders. To remain competitive, transit agencies must offer convenient, inexpensive, and quality service. Therefore, security measures that limit accessibility, cause delays, increase fares, or otherwise cause inconvenience could push people away from mass transit and back into their cars.

The size and diversity of the freight rail system make it difficult to adequately secure. The freight rail system's extensive infrastructure crisscrosses the nation and extends beyond our borders to move millions of tons of freight each day (see fig. 2.). There are over 100,000 miles of rail in the United States. The extensiveness of the infrastructure creates an infinite number of targets for terrorists.

Figure 2: Map of Class I Rail Lines



Source: GAO.

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

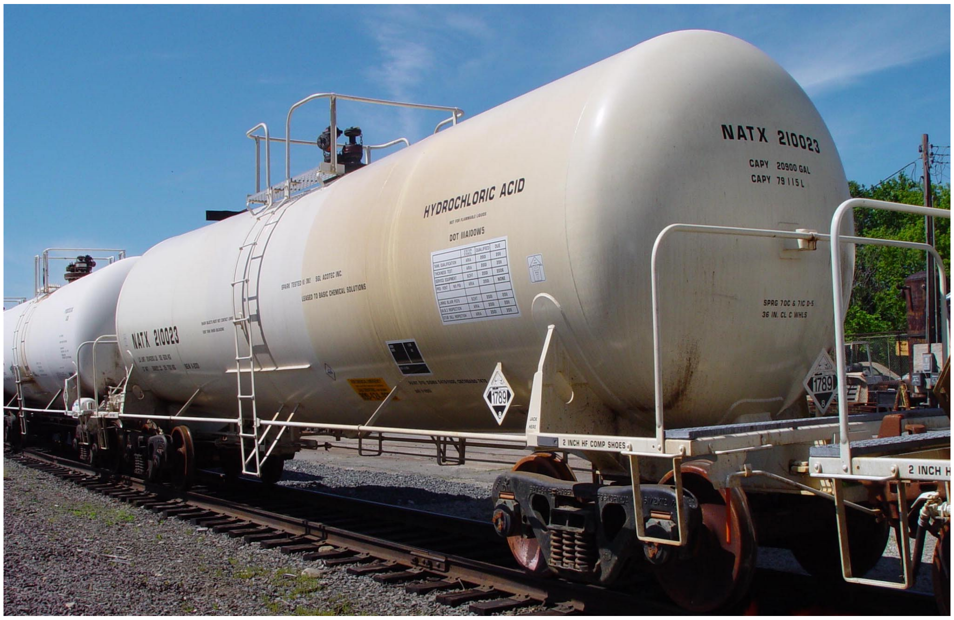
Protecting freight rail assets from attack is made more difficult because of the tremendous variety of freight hauled by railroads. For example, railroads carry freight as diverse as dry bulk (grain) and hazardous materials.[10] The transport of hazardous materials is of particular concern because serious incidents involving these materials have the potential to cause widespread disruption or injury. In 2001, over 83 million tons of hazardous materials were shipped by rail in the United States across the rail network, which extends through every major city as well as thousands of small communities. (Figure 3 is a photograph of a rail tanker car containing one of the many types of hazardous materials commonly transported by rail.) For our April 2003 report on rail security, we visited a number of local communities and interviewed federal and private

[10] Federal hazardous material transportation law defines a hazardous material as a substance or material that the Secretary of Transportation has determined is capable of posing an unreasonable risk to health, safety, and property when transported in commerce (49 U.S.C. § 5103). It includes hazardous substances such as ammonia, hazardous wastes from chemical manufacturing processes, and elevated temperature materials such as molten aluminum.

sector hazardous materials transportation experts.[11] A number of issues emerged from our work:

- the need for measures to better safeguard hazardous materials temporarily stored in rail cars while awaiting delivery to their ultimate destination--a practice commonly called "storage-in-transit,"
- the advisability of requiring companies to notify local communities of the type and quantities of materials stored in transit, and
- the appropriate amount of information rail companies should be required to provide local officials regarding hazardous material shipments that pass through their communities.

Figure 3: Hazardous Material Rail Tank Car



Source: Department of Homeland Security.

We recommended in April 2003 that DOT and DHS develop a plan that specifically addresses the security of the nation's freight rail infrastructure.[12] This plan should build

[11] GAO-03-435.

upon the rail industries' experience with rail infrastructure and the transportation of hazardous materials and establish time frames for implementing specific security actions necessary to protect hazardous material rail shipments. DHS has informed us that this plan is in progress.

Rail Stakeholders Have Taken Steps to Improve Security

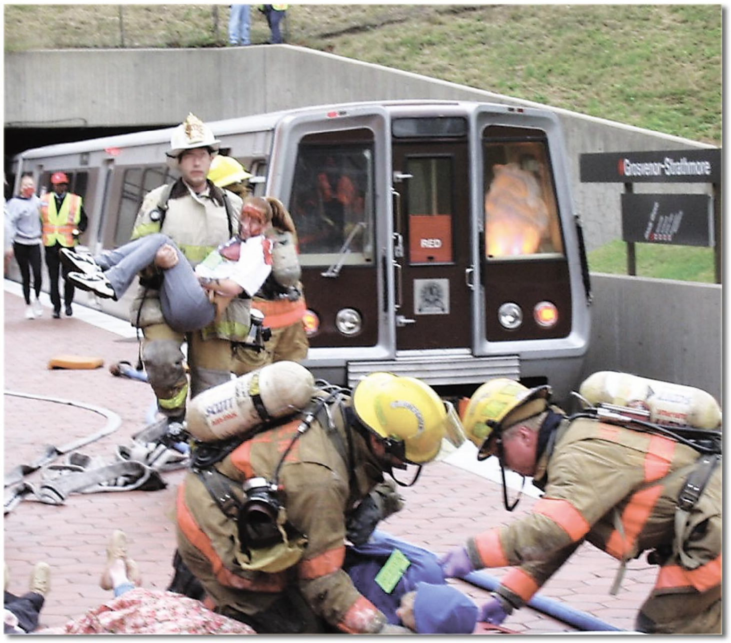
Since September 11, passenger and freight rail providers have been working to strengthen security. Although security was a priority before September 11, the terrorist attacks elevated the importance and urgency of transportation security for passenger and rail providers. According to representatives from the Association of American Railroads, Amtrak, and transit agencies, passenger and freight rail providers have implemented new security measures or increased the frequency or intensity of existing activities, including:

- **Conducted vulnerability or risk assessments:** Many passenger and freight rail providers 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.

- **Increased emergency drills:** Many passenger rail providers have increased the frequency of emergency drills. For example, as of June 2003, Amtrak had conducted two full-scale emergency drills in New York City. The purpose of emergency drilling is to test emergency plans, identify problems, and develop corrective actions. Figure 4 is a photograph from an annual emergency drill conducted by the Washington Metropolitan Area Transit Authority.

[12] GAO-03-435.

Figure 4: Emergency Drill in Progress



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

Source: GAO

- **Developed or revised security plans:** Passenger and freight rail providers developed security plans or reviewed existing plans to determine what changes, if any, needed to be made. For example, the Association of American Railroads worked jointly with several chemical industry associations and consultants from a security firm to develop the rail industry's security management plan. The plan establishes four alert levels and describes a graduated series of actions to prevent terrorist threats to railroad personnel and facilities that correspond to each alert level.

- **Provided additional training:** Many transit agencies have either participated in or conducted additional training on security or antiterrorism. For example, many transit agencies attended seminars conducted by FTA or by the American Public Transportation Association.

The federal government has also acted to enhance rail security. Prior to September 11, DOT modal administrations 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. In its first year of existence, TSA worked to establish its infrastructure and focused primarily on meeting the aviation security deadlines contained in ATSA. As TSA worked to establish itself and improve the security of the aviation system, DOT modal administrations, namely FRA, FTA, and RSPA, acted to enhance passenger and freight rail security (see tab. 1.). For example, FTA launched a multipart initiative for mass transit agencies that provided grants for emergency drills, offered free security training, conducted security assessments at 36 transit agencies, provided technical assistance, and invested in research and development. 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, including rail security. We reported in June 2003 that TSA was moving forward with efforts to secure the entire transportation system, such as developing standardized criticality, threat, and vulnerability assessment tools; and establishing security standards for all modes of transportation.[13]

Table 1: Key Actions Taken by DOT Modal Administrations to Help Secure the Rail System, September 2001 to May 2003

DOT modal administration	Security efforts
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.
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 transit agencies on security and emergency plans and emergency response drills. • Increased funding for security research and development efforts.
Research and Special Programs Administration	• 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

[13] GAO-03-843.

	hazmat community. • Published a 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 improves shipment security, and whether alternative methods for communicating safety hazards could be deployed.

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

Risk Management and Coordination Key to Enhancing Security

Although steps have been taken to enhance passenger and freight security since September 11, the recent terrorist attack on a rail system in Spain naturally focuses our attention on what more could be done to secure the nation's rail systems. In our previous work on transportation security, we identified future actions that the federal government could take to enhance security of individual transportation modes as well as the entire transportation system. For example, in our December 2002 report on mass transit security, we recommended that the Secretary of Transportation seek a legislative change to give mass transit agencies more flexibility in using federal funds for security-related operating expenses, among other things.[14] Two recurring themes cut across our previous work in transportation security—the need for the federal government to utilize a risk management approach and the need for the federal government to improve coordination of security efforts.

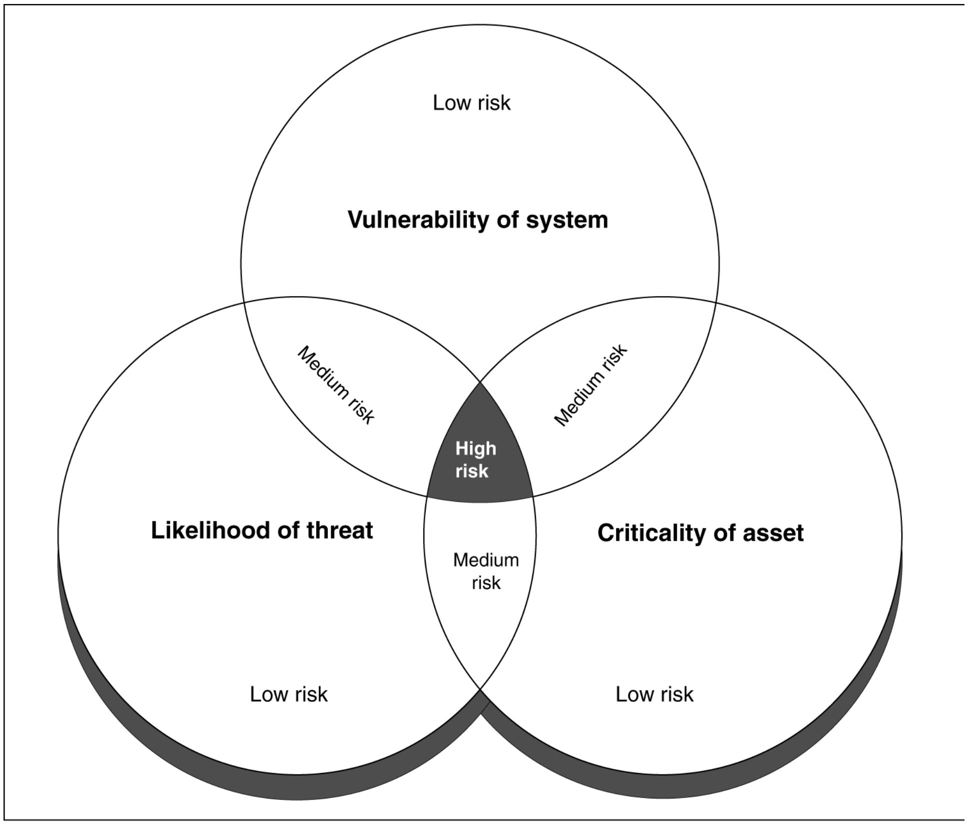
Using risk management principles to guide decision-making is a good strategy, given the difficult trade-offs the federal government will likely have to make as it moves forward with its transportation security efforts. We have advocated using a risk management approach to guide federal programs and responses to better prepare against terrorism and other threats and to better direct finite national resources to areas of highest priority.[15] As figure 5 illustrates, the highest priorities emerge where threats,

[14] GAO-03-263. DOT agreed to carefully consider our recommendations as it moved forward with its efforts to improve transit security.

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

vulnerabilities, and criticality overlap. For example, rail 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. The federal government is likely to be viewed as a source of funding for at least some rail security enhancements. These enhancements will join the growing list of security initiatives competing for federal assistance. A risk management approach can help inform funding decisions for security improvements within the rail system and across modes.

Figure 5: Representation of Risk



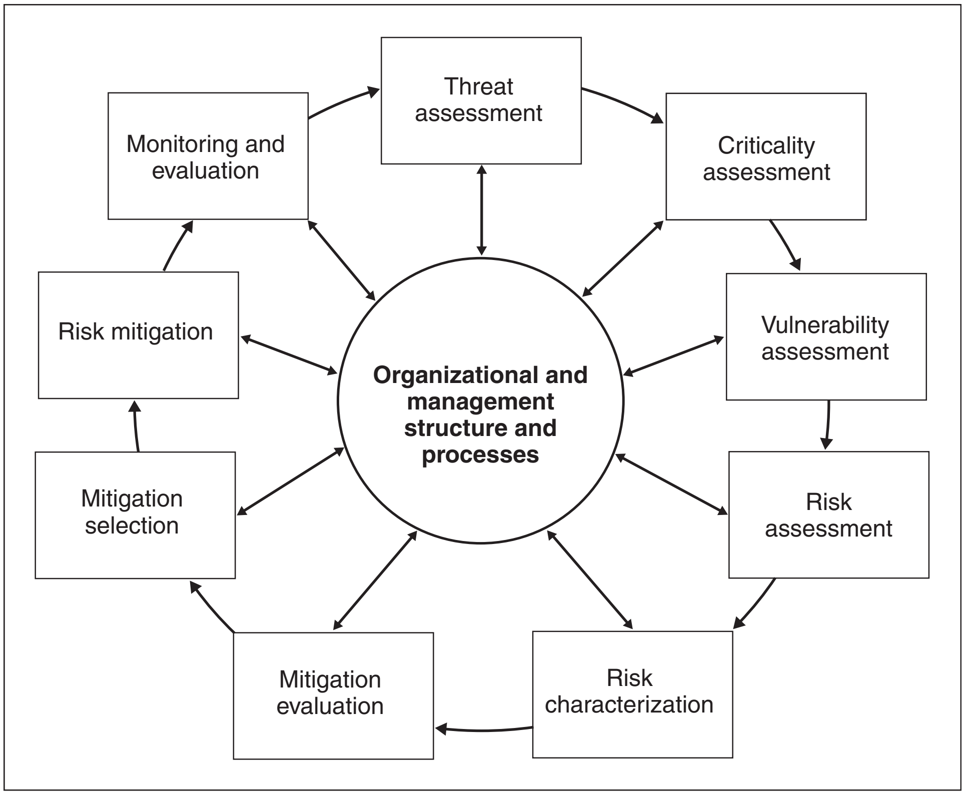
Source: GAO.

A risk management approach entails a continuous process of managing, through a series of mitigating actions, the likelihood of an adverse event happening with a negative

Threat and Risk Assessments Can Help Prioritize and Target Program Investments, GAO/NSIAD-98-74 (Washington, D.C.: April 9, 1998).

impact. Risk management encompasses “inherent” risk (i.e., risk that would exist absent any mitigating action), as well as “residual” risk (i.e., the risk that remains even after mitigating actions have been taken). Figure 6 depicts the risk management framework. Risk management principles acknowledge that while risk cannot be eliminated, enhancing protection from known or potential threats can help reduce it. (Appendix I provides a description of the key elements of the risk management approach.) We reported in June 2003 that TSA planned to adopt a risk management approach for its efforts to enhance the security of the nation’s transportation system. According to TSA officials, risk management principles will drive all decisions—from standard-setting, to funding priorities, to staffing.

Figure 6: Risk Management Framework



Source: GAO analysis.

Coordination is also a key action 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 such problems 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."

We reported in June 2003 that the roles and responsibilities of TSA and DOT in transportation security, including rail security, have yet to be clearly delineated, which creates the potential for duplicating or conflicting efforts as both entities work to enhance security. Legislation has not defined TSA's role and responsibilities in securing all modes of transportation. 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. Instead, the act simply states that TSA is responsible for ensuring security in all modes of transportation. The act also did not 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 the roles and responsibilities of TSA and DOT in transportation security matters, we recommended 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. The Department of Homeland Security (DHS) and DOT disagreed with our recommendation, noting that DHS had the lead for the Administration in transportation security matters and that DHS and DOT were committed to broad and routine consultations. We continue to believe our recommendation is valid. A mechanism, such as a memorandum of agreement, would serve to clarify, delineate, and document the roles and responsibilities of each entity. This is especially important considering DOT responsibilities for transportation safety overlap with DHS' role in securing the transportation system. Moreover, recent pieces of legislation give DOT transportation security responsibilities for some activities, including the rail security. Consequently, the lack of clearly delineated roles and responsibilities could lead to duplication, confusion, and gaps in preparedness. A mechanism 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.

Observations

Securing the nation's passenger and freight rail systems is a tremendous task. Many challenges must be overcome. Passenger and freight rail stakeholders have acted to enhance security, but more work is needed. As passenger and freight rail stakeholders, including the federal government, work to enhance security, it is important that efforts be coordinated. The lack of coordination could lead to duplication and confusion. More importantly, it could hamper the rail sector's ability to prepare for and respond to attacks. In addition, to ensure that finite resources are directed to the areas of highest priority, risk management principles should guide decision-making. Given budget pressures at all levels of government and the sluggish economy, difficult trade-offs will undoubtedly need to be made among competing claims for assistance. A risk management approach can help inform these difficult decisions.

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

Contacts and Acknowledgments

For information about this testimony, please contact Peter Guerrero, Director, Physical Infrastructure Issues, on (202) 512-2834; or Norman Rabkin, Managing Director, Homeland Security and Justice Issues, on (202) 512- 8777. Individuals making key contributions to this testimony included Nikki Clowers, Susan Fleming, Maria Santos, and Robert White.

Appendix I: Key Elements of a Risk Management Approach

Threat Assessment. Threat is defined as potential intent to cause harm or damage to an asset (e.g., natural environment, people, man-made infrastructures, and activities and operations). A threat assessment identifies adverse events that can affect an entity and may be present at the global, national, or local level.

Criticality assessment. Criticality is defined as an asset's relative worth. A criticality assessment identifies and evaluates an entity's assets based on a variety of factors, including importance of a function and the significance of a system in terms of national security, economic activity, or public safety. Criticality assessments help to provide a basis for prioritizing protection relative to limited resources.

Vulnerability assessment. Vulnerability is defined as the inherent state or condition of an asset that can be exploited to cause harm. A vulnerability assessment identifies the extent that these inherent states may be exploited, relative to countermeasures that have been or could be deployed.

Risk Assessment. Risk assessment is a qualitative and/or quantitative determination of the likelihood of an adverse event occurring and the severity, or impact, of its consequences. It may include scenarios under which two or more risks interact, creating greater or lesser impacts, as well as the ranking of risky events.

Risk characterization. Risk characterization involves designating risk on a categorical scale (e.g., low, medium, and high). Risk characterization provides input for deciding which areas are most suited to mitigate risk.

Mitigation Evaluation. Mitigation evaluation is the identification of mitigation alternatives to assess the effectiveness of the alternatives. The alternatives should be evaluated for their likely effect on risk and their cost.

Mitigation Selection. Mitigation selection involves a management decision on which mitigation alternatives should be implemented among alternatives, taking into account risk, costs, and the effectiveness of mitigation alternatives. Selection among mitigation alternatives should be based upon pre-considered criteria. There are as of yet no clearly preferred selection criteria, although potential factors might include risk reduction, net benefits, equality of treatment, or other stated values. Mitigation selection does not necessarily involve prioritizing all resources to the highest risk area, but in attempting to balance overall risk and available resources.

Risk mitigation. Risk mitigation is the implementation of mitigating actions, depending upon an organization's chosen *action posture* (i.e. the decision on what to do about overall risk). Specifically, risk mitigation may involve risk acceptance (taking no action), risk avoidance (taking actions to avoid activities that involve risk), risk reduction (taking actions to reduce the likelihood and/or impact of risk), and risk sharing (taking actions to reduce risk by sharing risk with other entities). As shown in figure 6, risk mitigation is best framed within an integrated systems approach that encompasses action in all organizational areas; including personnel, processes, technology, infrastructure, and governance. An integrated systems approach helps to ensure that taking action in one or more areas would not create unintended consequences in another area.

Monitoring and evaluation. Monitoring and evaluation is a continuous repetitive assessment process to keep risk management current and relevant. It should involve reassessing risk characterizations after mitigating efforts have been implemented. It also includes peer review, testing, and validation.