S. HRG. 109–462

DOMESTIC PASSENGER AND FREIGHT RAIL SECURITY

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

OCTOBER 20, 2005

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

28–172 PDF WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

TED STEVENS, Alaska, *Chairman*

JOHN McCAIN, Arizona
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
GORDON H. SMITH, Oregon
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia
JOHN E. SUNUNU, New Hampshire
JIM DeMINT, South Carolina
DAVID VITTER, Louisiana

DANIEL K. INOUYE, Hawaii, *Co-Chairman*
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
E. BENJAMIN NELSON, Nebraska
MARK PRYOR, Arkansas

LISA J. SUTHERLAND, *Republican Staff Director*
CHRISTINE DRAGER KURTH, *Republican Deputy Staff Director*
DAVID RUSSELL, *Republican Chief Counsel*
MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*
SAMUEL E. WHITEHORN, *Democratic Deputy Staff Director and General Counsel*
LILA HARPER HELMS, *Democratic Policy Director*

CONTENTS

DOMESTIC PASSENGER AND FREIGHT RAIL SECURITY

THURSDAY, OCTOBER 20, 2005

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington DC.

The Committee met, pursuant to notice, at 10 a.m. in room SD–562, Dirksen Senate Office Building, Hon. Ted Stevens, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. TED STEVENS, U.S. SENATOR FROM ALASKA

The CHAIRMAN. Good morning.

Mr. HAWLEY. Good morning, Mr. Chairman.

The CHAIRMAN. I welcome you here today and I want to thank you for your willingness to appear before the Committee to discuss the security of our Nation's rail system. Alaska, has only one railroad, as you know. As a matter of fact, it's really essential to our livelihood and it has an interesting history, which I won't go into now. This is one of a series of hearings we're going to hold, to try and fulfill our oversight responsibilities on TSA, to work to develop our understanding of the security systems that are going to be implemented for all modes of transportation. I hope that we can get other Senators here to explore some of the details that are involved here, in your reports. I have gone through them briefly, but, I'm very interested in pursuing the whole subject.

We have a report here from GAO that I find very interesting and it indicates there remains confusion among the various entities, as to who is actually in charge of the initiatives that are necessary to improve rail security. So, I look forward to your testimony. I'm going to put my statement in full in the record and will give a similar opportunity for all the members, to put their statements in the record.

[The prepared statement of Senator Stevens follows:]

PREPARED STATEMENT OF HON. TED STEVENS, U.S. SENATOR FROM ALASKA

I welcome the witnesses who are here today and I thank you for your willingness to appear before the Committee to discuss the security of our Nation's rail system, a matter that is essential to the preservation of interstate commerce and the U.S. economy. In my State of Alaska, freight and passenger rail lines are a vital means of transportation for resources, as well as tourism. The Alaska Railroad Corporation hauls 7 million tons of freight and 500,000 passengers each year, and employs more than 700 Alaskans.

Today's hearing is one in a series of hearings that the Committee will hold to fulfill its oversight responsibilities over the Transportation Security Administration (TSA) as we work to develop ways to further improve the security of all modes of transportation, including our rail systems.

However, in securing any mode of transportation, we must achieve a balance in our approach that ensures the greatest security possible while not inhibiting the free flow of commerce. Senator Inouye and I, along with several of our Committee colleagues, have attempted to achieve that balance in legislation that we introduced that addresses the security of all modes, including the security of our rail systems.

Much has been done since September 11th to enhance the security of our Nation's rail systems, particularly by the freight and passenger rail industries, which have invested substantially to ensure the security of their infrastructure and assets. But the London bombings and the recent threats to the New York City subway system underscore the fact that much more remains to be done.

Despite TSA being designated the lead agency with authority over rail security nearly four years ago, the agency has been criticized by the Government Accountability Office and the rail industry for not seeking industry input in policy decisions, and for not acting quickly enough to assess risk and allocate resources. GAO recently reported that TSA has yet to finalize risk assessments of passenger rail systems around the country, or set a time-line for the completion of such assessments. GAO indicated that there remains confusion among stakeholders concerning who is actually in charge given that several Federal agencies have initiatives to improve rail security.

I welcome Mr. Hawley's testimony on these topics, and I look forward to a constructive dialogue concerning ways to enhance rail security.

Our first witness today, is the Assistant Secretary of the Transportation Security Administration, Kip Hawley. I am pleased to have your statement, Mr. Hawley.

STATEMENT OF EDMUND "KIP" HAWLEY, ASSISTANT SECRETARY, TRANSPORTATION SECURITY ADMINISTRATION

Mr. HAWLEY. Thank you, Mr. Chairman and good morning. I appreciate my first opportunity to appear as head of the TSA before this Committee and this morning, I will discuss our efforts to assure domestic passenger and freight rail security.

At the outset, I want to acknowledge the team nature of security in today's world and express appreciation for the Government Accountability Office and Cathy Berrick, who's represented on this panel and the Department of Transportation today, represented by Federal Railroad Administrator, Joe Boardman.

America's passenger and freight transportation system is a dynamic, interconnected network. It consists of overlapping sub-networks and multiple organizations, with a variety of governance structures and a mix of public and private ownership. In terms of security, decentralized systems such as this are more difficult to "secure," but they also have advantages. They present more operational uncertainty to those who would do them harm, and they are more robust in the face of catastrophic failure of any single component of the network.

Despite the good work that has already been done to improve security and transit, the London bombings and other events throughout the world have demonstrated the need for a refined approach to transportation security.

Fundamentally, our challenge is to protect our transportation networks in a constantly changing threat environment. We understand better that terrorists will not only look for weaknesses in our transportation system and in security measures, but they will also adapt to perceived security measures. As a result, it is not possible to precisely "predict", with any degree of certainty, the next attack based on previous terrorist activity. In the face of unpredictability and rapid change with respect to threats, our approach to security in every transportation sector must be based on flexibility and adaptability.

While it is necessary, it is no longer sufficient to protect ourselves against known or suspected terrorists; we must protect ourselves against people with no known affiliation to terrorism.

While it is necessary, it is no longer sufficient to focus on finding threat devices like guns, explosives and knives, we must enhance our ability to find terrorists before an attack is underway.

And while it is necessary, but no longer sufficient to subject every passenger to basic security procedures, we must create uncertainty and an element of unpredictability in security operations in order to disrupt terrorist planning and attempts.

To accomplish these objectives, TSA is pursuing a security strategy based on Security Chair Chertoff's Second Stage Review. There are four core operating principles applicable to TSA. First, we will use analysis based on risk, vulnerability and consequence to make investment and operational decisions. Second, we will avoid giving terrorists an advantage based on our predictability. TSA will deploy resources, canine teams, air marshals, or inspectors, for example and establish protocols, standards and best practices, flexibly based on risk. Terrorists will not be able to use the predictability of our security measures to their advantage in planning or carrying out an attack. Third, we will continue to intervene early based on intelligence, law enforcement information and counter-surveillance suspicious incident reporting, to focus our security measures on the terrorist, as well as the means for carrying out the threat. Effective analysis and dissemination of timely information to those who need them is a vital component of this effort.

Finally, we will build and take advantage of security networks. We are pursuing a restructuring of TSA that will put a renewed emphasis on building information sharing networks in every transportation sector. Through these efforts, we work more closely with stakeholders and put a renewed emphasis on sharing intelligence, capacity and technology with other law enforcement, intelligence gathering and security agencies at every level of government. As we move forward, we are fortunate to be able to build upon a solid foundation of work, not only at the local level, but nationally as well. This foundation includes products and resources, developed by our Federal partners, especially the Department of Transportation, with the Federal Transit Administration and the Federal Railroad Administration, and partners in industry, such as the American Public Transportation Association, the Association of American Railroads and its members, labor unions and individual public transportation systems.

This collective experience fortifies our knowledge, expertise and overall strategic approach. We value the critical role that Congress, and especially this Committee, plays in the effort. We look forward to working with you on the full range of these issues. I'll be happy to answer any questions at the appropriate time.

[The prepared statement of Mr. Hawley follows:]

PREPARED STATEMENT OF EDMUND "KIP" HAWLEY, ASSISTANT SECRETARY, TRANSPORTATION SECURITY ADMINISTRATION

Good morning, Mr. Chairman, Co-Chairman Inouye, and Members of the Committee. I am pleased to have this opportunity to testify on the subject of domestic passenger and freight rail security.

At the outset, I acknowledge and appreciate the work of the Government Accountability Office (GAO) in its recent report on passenger rail security. The strategic approach, programs, and initiatives I will discuss today move us well along in addressing the GAO's recommendations.

As you know, the September 11 attacks focused Congress, the Administration, and the public on improving the security of our aviation system. It was an honor to be a part of the team that helped create the Transportation Security Administration (TSA) at the Department of Transportation (DOT), and it is an honor today to have the opportunity to lead the agency at the Department of Homeland Security, as we refocus and realign TSA to reflect the changing reality of terrorist threats to the transportation sector. Of necessity, much of our early work at TSA focused on the very real and present threats and vulnerabilities in aviation. We were fortunate to have partners at DOT and in industries and communities around the Nation who immediately stepped forward at that time to initiate security improvements in the transit and rail sectors. Today, we continue to work with these partners and build upon their record of success to address the changing transportation threat environment.

Overview of Surface Transportation

America's passenger and freight transportation system is a dynamic, interconnected network. It consists of overlapping sub-networks and multiple organizations, with a variety of governance structures and a mix of public and private ownership. In terms of security, decentralized systems such as this are more difficult to "control," but they also have advantages. They present more operational uncertainty to those who seek to do them harm, and they are more robust in the face of catastrophic failure of any single component of their networks.

Public Transportation. America's public transportation system is actually composed of over 6,000 separate local transit systems. These local systems range from very small bus-only systems in rural communities, to very large multi-modal systems in urban areas that may combine bus, light rail, subway, commuter rail and ferry operations. Transit systems are not only locally operated, but they are also protected largely by State and local law enforcement.

Americans took 9.4 billion trips using public transportation in 2003. The 30 largest transit systems in the U.S. carry most (almost 80 percent) of the Nation's transit passenger trips. There is now some form of rail transit (light rail, subway, or commuter rail) operated by 53 different transit agencies located in 33 cities and 23 states. These rail systems provide a combined 11.3 million passenger trips each weekday, compared to 1.8 million domestic emplanements per day nationwide.

Approximately 28 percent of all transit trips and 77 percent of all rail transit trips are on heavy rail. There are 14 heavy rail transit systems (also known as subways) in the U.S., consisting of more than 2,000 route miles, with over 1,000 stations and approximately 10,500 subway cars. The New York City subway system is the largest in the U.S., carrying about 75 percent of the Nation's heavy rail passengers, with half of the stations and more than 6,000 scheduled trains per day carrying over 3 million riders. In New York's Penn Station alone, more than 1,600 people *per minute* pass through dozens of access points during a typical rush hour.

Intercity Bus Transportation. Though not owned by public entities, intercity bus service is an important component of America's transportation network. Intercity bus service is provided by over 4,000 private operators across the country, 90 percent of which operate 25 or fewer buses. Greyhound is the largest intercity bus operator, with a fleet of more than 2,400 buses. Public transit buses annually carry about 8 times the number of riders as intercity buses; heavy rail (subway) operators carry over 3 times as many riders as intercity buses.

Intercity Passenger Rail. Intercity passenger rail service is provided by two entities: Amtrak and the Alaska Railroad Corporation (ARRC), which is a public corporation of the State of Alaska. The ARRC provides freight and passenger service from Whittier, Seward and Anchorage to Fairbanks, Denali National Park and military installations.

Amtrak carries approximately 25 million passengers per year or an estimated 68,000 passengers per day, operating as many as 300 trains per day and serving over 500 stations in 46 States. In many large cities, Amtrak stations are co-located with stations serving rail transit, intercity bus, and other modes of transportation.

Amtrak operates over more than 22,000 route miles. It owns 650 route miles, primarily between Boston and Washington, D.C., and in Michigan. In other parts of the country, Amtrak trains use tracks owned by freight railroads.

Freight Rail. U.S. freight railroads operate over a network spanning more than 140,000 route miles. This system is vital to the economy, linking businesses and ensuring products reach consumers in an efficient, safe, and cost-effective manner. Still, recent events, such as the accidental derailment in Graniteville, SC, that resulted in the release of chlorine gas, have highlighted the need to focus additional attention on the potential security risks associated with freight rail. Over 64 percent of toxic inhalation hazard chemicals are currently transported by rail. In 2003, over 60,000 tank cars of chlorine or anhydrous ammonia chemicals were shipped, each carrying an average of 90 tons of chlorine or 30,000 gallons of anhydrous ammonia.

London Lessons Learned

Al-Qaeda and its affiliated extremist groups and sympathizers demonstrated their ability to strike mass transit targets with suicide bombings on buses in Israel, Turkey and China, and bombings of subways, rail systems, and ferries in India, Pakistan, Thailand, Chechnya, Russia and the Philippines. The Madrid train attacks in 2004 and the London subway and bus attacks on July 7 and 21 of this year have further reminded us that our trains, subways and buses may be terrorist targets.

Heavy rail transit systems in the U.S., like the London Underground, are particularly high consequence targets in terms of potential loss of life and economic disruption. These systems carry large numbers of people in a confined environment, offer the potential of targeting specific populations at particular destination stations, and often have stations located below or adjacent to high profile government buildings, major office complexes, or public icons. Threats to particular economic sectors, like government or financial institutions, may also be carried out through attacks on public transit.

The London attacks were particularly noteworthy from a security perspective.

- In a relatively short period of time, unknown and apparently unaffiliated individuals/groups were able to plan and execute the attacks with little or no surveillance or rehearsal activity.
- The perpetrators came through fare-gates directly onto the train; they did not access storage yards, tunnels or bridges. As a result, London's extensive intrusion detection devices and security cameras did not prevent the attacks. Recording capability was helpful, but only after-the-fact in helping to identify suspects.
- The improvised explosive devices used by the attackers were assembled with materials readily available in local shops. The devices fit easily into backpacks of the type and design commonly carried by students, commuters, and tourists.
- Even with markedly increased public awareness, countermeasures, and law enforcement presence after the first London bombings, the same methods were able to be used in the second attack without suspicion or detection.

Immediately following the first London attacks, transit agencies and local officials took action. Responding to a joint inquiry by TSA and DOT's Federal Transit Administration (FTA), the 30 largest transit agencies reported that they:

- Extended patrol hours through law enforcement overtime and the deployment of administrative and operational personnel;
- Expanded the use of canine explosive detection patrols; and
- Issued more frequent and more detailed public awareness announcements regarding how to report unattended bags and suspicious behavior and how to evacuate from particular transit environments (i.e., train cars, tunnels, and bridges).

These actions built upon the important security foundation that was established over the last several years. In contrast to their pre-9/11 security posture, all of the largest transit agencies have now: developed and implemented action plans that are specific to each Homeland Security Alert System threat level; sent front-line employees to Federally-funded security and emergency response training courses; instituted public awareness campaigns, many utilizing Federally-developed materials; developed and tested emergency response plans; and hardened numerous assets to protect against security threats.

Adapting to a Changing Threat Environment

Despite the work that has already been done, Mr. Chairman, the London bombings and other events throughout the world have demonstrated the need for a new strategic approach to transportation security. Fundamentally, our challenge is to protect passengers, freight, and our transportation network in a constantly changing threat environment. We understand better that terrorists will not only look for weaknesses in our transportation system and its security measures, but they will also adapt to perceived security measures. As a result, it is not possible to "predict" the next attack based on previous terrorist activity or put into place specific security measures to protect against it. In this dynamic environment, history is an unreliable guide.

In the face of unpredictability and rapid change in terms of threats, our approach to security in every transportation sector must be based on flexibility and adaptability.

- While it is *necessary,* it is no longer *sufficient* to protect ourselves against known or suspected terrorists; we must protect ourselves against people with no known affiliation to terrorism.
- While it is *necessary,* it is no longer *sufficient* to focus on finding weapons and common explosives; we must enhance our ability to recognize suspicious behavioral patterns and demeanors to identify people who may have devised a new means to attack our transportation systems or passengers.
- While it is *necessary,* it is no longer *sufficient* to subject every passenger to the same basic security procedures; we must create uncertainty and an element of randomness in security operations in order to disrupt terrorist planning and attempts.
- While it is *necessary,* it is no longer *sufficient* to focus solely on identifying the actors, like suicide bombers; we must integrate our security measures with local law enforcement to identify those who make the bombs and provide support.

Therefore, TSA is pursuing a security strategy based on Secretary Chertoff's Second Stage Review, the National Strategy for Transportation Security, and the following four operating principles:

First, we will use risk/value analysis to make investment and operational decisions. That means that we will assess risks based not only on threat and vulnerability, but on the potential consequences of a particular threat to people, transportation assets, and the economy. Further, we will assess and undertake risk management and risk mitigation measures based on their effect on total transportation network risk. This holistic approach to risk assessment and risk mitigation may lead us, for example, to redirect the actions of our airport screeners to focus less on identifying and removing less threatening items from carry-on luggage, so that their time and attention can be spent on identifying potential components of an improvised explosive device.

Second, we will avoid giving terrorists or potential terrorists an advantage based on our predictability. TSA will deploy resources—whether they are canine teams, screeners, air marshals, or inspectors—and establish protocols flexibly based on risk, so that terrorists cannot use the predictability of security measures to their advantage in planning or carrying out a threat. This may mean changing or adding to inspection routines on a daily or hourly basis to introduce uncertainty into terrorist planning efforts.

Third, we will continue to intervene early based on intelligence, and focus our security measures on the terrorist, as well as the means for carrying out the threat. Enhancing and expanding the techniques to identify suspicious persons at the transit, train, or bus station, or to detect explosive devices is necessary. However, the strongest defense posture detects the terrorist well before the attempt to launch an attack has begun. A coordinated interagency intelligence collection and analysis effort must stand as the first line of defense. Effective dissemination of timely intelligence products to those who need them is a vital component of this effort.

And, finally, we will build and take advantage of security networks. As you may know, I am pursuing a restructuring of TSA that will put a renewed emphasis on building information sharing networks in every transportation sector—rail, transit, maritime, and trucking, as well as aviation. Not only will we work more closely with stakeholders in these industries, we will put a renewed emphasis on sharing intelligence, capacity and technology with other law enforcement, intelligence gathering and security agencies at every level of government. We will build a more robust, distributed network of security systems to protect America.

As we apply these operational principles, I have also directed my staff to rededicate themselves to important customer service principles, as well. As we move forward:

- TSA will identify opportunities and engage the private sector in its work to develop and implement security systems and products.

- We will protect the privacy of Americans by minimizing the amount of personal data we acquire, store and share, and we will vigorously protect any data that is collected, stored or transmitted.
- And TSA will remember, in all that we do, our goal in stopping terrorism is to protect the freedoms of the American people. Therefore, we will work to make travel easier for the law-abiding public, while protecting the security of the transportation network and the people who depend upon it.

A Solid Foundation

As we move forward strategically to enhance our security efforts in the public transportation and rail sectors, we are fortunate to be able to build upon a solid foundation of work, not only at the local level, but nationally, as well.

Grants. Substantial Federal assistance has been and will continue to be provided to support improved transit and rail security. TSA has assisted the DHS Office of State and Local Government Coordination and Preparation (SLGCP) in the development of its Transit Security Grant Program (TSGP). To date, SLGCP has provided more than $255 million to State and local transit agencies through this program to increase protection through hardening of assets, greater police presence during high alerts, additional detection and surveillance equipment, increased inspections, and expanded use of explosives detection canine teams. In April 2005, DHS announced $141 million in TSGP funding, of which more than $107 million has been dedicated to owners and operators of rail systems. An additional $6 million was awarded to Amtrak through the Inter-city and Passenger Rail Security Program (IPRSGP) for security enhancements to passenger rail operations in the Northeast Corridor and at Amtrak's hub in Chicago. Additionally, through SLGCP's State Homeland Security Grant Program and Urban Area Security Initiative, the Department has allocated more than $8.3 billion for general counterterrorism preparedness.

The FY 2006 appropriations bill includes an additional $2.5 billion for this purpose. The bill also includes a total of $390 million in discretionary grants specifically for surface transportation security programs, including $150 million for rail and transit security, $175 million for port security, $10 million for intercity bus security, and $5 million for the Highway Watch program. TSA will continue to work closely with SLGCP on these programs, as well.

Security Exercises and Training. TSA has held numerous security exercises that bring together stakeholders, Federal, State, and local first responders, and security experts to test preparedness and response and identify best practices and lessons learned. We are also seeking new and improved ways to exercise and train for prevention methods, which will help strengthen a national prevention capability. These efforts will develop and support effective relationships among Federal, State and local entities and the private sector, and they significantly enhance our ability to anticipate and respond quickly and appropriately to security issues.

Additionally, through an interagency agreement with the Federal Law Enforcement Training Center (FLETC), TSA has trained over 400 law enforcement officers, transit police, and first responders through the Land Transportation Anti-Terrorism Training Program. TSA has also contracted with the FTA's National Transit Institute to develop a CD-ROM-based interactive training program for passenger and freight rail employees. This product is expected to be completed before the end of the current fiscal year. These training programs emphasize antiterrorism planning and prevention for land transportation systems. Areas of focus include security planning, transit system vulnerabilities, contingency planning, recognition and response for threats involving explosives and weapons of mass destruction, and crisis and consequence management. Guest instructors with specialized expertise supplement the FLETC staff, providing the benefit of actual experience through case studies.

Self-Assessment Tool. TSA has developed the Vulnerability Identification Self-Assessment Tool (VISAT), a multi-modal tool that public transportation agencies may voluntarily use to self-assess vulnerabilities within their systems. Specific modules focus on mass transit (heavy rail/subways), rail passenger stations, highway bridges, maritime, and operations centers. Additional modules under development will ensure this tool covers the spectrum of modes for which TSA holds lead responsibility for security. In general, the tool focuses on the prevention and the mitigation of an array of threat scenarios developed for each mode within the sector. Users rate their entity in terms of target attractiveness (from a terrorist's perspective) and several consequence categories that broadly describe health and well-being, economic consequence, and symbolic value of the entity. The tool enables a user to capture a snapshot of its security system baseline, assessing vulnerabilities in the system and assisting in the development of a comprehensive security plan.

Surface Transportation Security Inspector Program. The Department of Homeland Security Appropriations Act for FY 2005 provided $12 million to TSA for rail security, including $10 million to deploy 100 Federal security compliance inspectors and Congress has continued this funding in FY 2006. TSA has made substantial progress in developing a robust and comprehensive surface transportation security compliance inspector program with emphasis on hiring, training, and logistical and procedural planning. A total of 99 inspectors are now on board. Among other tasks, the security compliance inspectors will identify gaps in security and validate compliance with TSA's security directives.

Conclusion

Mr. Chairman and Members of the Committee, I want to assure you that TSA is pursuing a robust strategy to support rail and transit security that builds upon the work of other Department of Homeland Security agencies, the Department of Transportation, and our public and private sector partners at the State and local level. We value the critical role the Congress, and especially this Committee, plays in this effort. The success of Secretary Chertoff's Second Stage Review and the strategic approach I've described today depend upon retaining the flexibility to determine risk-based priorities and to adjust our tactics to respond to developing circumstances and emerging trends. We look forward to working with Congress and this Committee on the full range of subjects so critical to protecting America's transportation infrastructure, its passengers, and the commerce that depends upon it.

Thank you. I would be pleased to respond to questions.

The CHAIRMAN. Thank you very much. Senator McCain, do you have an opening statement?

Senator MCCAIN. Since you've already begun, I'd be glad to wait until after the witnesses, Mr. Chairman.

The CHAIRMAN. Well, thank you. Our next witness is the Administrator of the FRA, Mr. Joseph Boardman.

STATEMENT OF JOSEPH H. BOARDMAN, ADMINISTRATOR, FEDERAL RAILROAD ADMINISTRATION

Mr. BOARDMAN. Good morning, Mr. Chairman, Senator McCain, other Members of the Committee, I am pleased to be here today to testify, on behalf of the Secretary of Transportation, about the security of our Nation's passenger and freight railroad network.

Since June 1 of this year, it has been my privilege to serve as the Administrator of the Federal Railroad Administration.

Although DOT has not yet prepared a views report on Senate 1052, which precludes me from providing official views on the provisions of that bill, we're certainly willing to work with this Committee on any legislative ideas that will enhance rail security.

The FRA administers the Federal Railroad Safety Laws, which provide FRA with authority over every area of railroad safety. It also enforces hazardous material transportation regulations issued by PHMSA or the Pipeline and Hazardous Materials Safety Administration. And although the railroad industry's overall safety record has improved over the last decade and most safety trends are moving in the right direction, significant train accidents continue to occur.

As a result, in May of 2005, Secretary Mineta announced a Railroad Safety Action Plan and FRA has begun to move forward on all elements of that action plan. FRA has a role in transportation railroad security. To date, FRA personnel have reviewed security plans, and security training records, and since April of 2004, FRA and PHMSA have also worked with DHS on a coordinated plan to improve the security of the rail transport of hazardous materials classified as "Toxic Inhalation Hazards." In the area of passenger security, FRA inspectors have conducted basic security reviews of Amtrak and commuter railroads, in work with TSA inspectors after the July transit bombings in London, together, to ensure safety in passenger service.

FRA sponsors and conducts research, development and technology demonstrations that are related to rail security through its Office of Research and Development such as exploring various methods to harden tank cars.

In September 2004, DOT and DHS entered into a Memorandum of Understanding concerning their respective roles on security issues. The MOU requires early coordination between the parties on the development of regulations affecting security and will help delineate each department's specific area of responsibility.

FRA works closely with the managers of the Transportation Security Administration's new Rail Security Inspection Program. A day to day connection with that is extremely important for the event of catastrophic events. FRA's primary mission is helping to ensure the safety of railroad transportation. In some areas such as hazardous material transportation, safety and security are inextricably intertwined, which means that FRA safety activities will no doubt continue to have an effect on security. In general, however, FRA's role is to support DHS and TSA in carrying out their security responsibilities to the extent FRA can do so within its present authority and with its current resources.

Thank you and I'm available for questions.

[The prepared statement of Mr. Boardman follows:]

PREPARED STATEMENT OF JOSEPH H. BOARDMAN, ADMINISTRATOR, FEDERAL RAILROAD ADMINISTRATION

Chairman Stevens, Ranking Member Inouye, and other Members of the Committee, I am very pleased to be here today to testify, on behalf of the Secretary of Transportation, about the security of our Nation's passenger and freight railroad network. Since June 1 of this year, it has been my privilege to serve as the Administrator of the Federal Railroad Administration (FRA). By delegation from the Secretary, FRA's primary mission is to promote the safety of the U.S. railroad industry and to reduce the number and severity of accidents and incidents arising from railroad operations. Our railroad safety mission necessarily includes our involvement in railroad security issues. The U.S. Department of Homeland Security (DHS) has the primary responsibility for transportation security. FRA plays a supporting role, providing technical assistance and assisting DHS when possible with implementation of its security policies, as allowed by statutory authority and available resources

My testimony today will provide some background on FRA's railroad safety program and briefly describe the role that FRA plays in railroad security.

FRA's Railroad Safety Program

FRA administers the Federal railroad safety laws, which provide FRA with authority over "every area of railroad safety," 49 U.S.C. 20103(a). The agency has issued a wide range of safety regulations covering such topics as: track; passenger equipment; locomotives; freight cars; power brakes; locomotive event recorders; signal and train control systems; maintenance of active warning devices at highway-rail grade crossings, accident reporting, alcohol and drug testing, protection of roadway workers; operating rules and practices; locomotive engineer certification; positive train control; and use of train horns at grade crossings. We currently have active rulemaking projects on a number of important safety topics, including locomotive crashworthiness, noise exposure of railroad employees, and continuous welded rail. In addition, FRA enforces hazardous materials regulations issued by another DOT agency, the Pipeline and Hazardous Materials Safety Administration (PHMSA). Those regulations include requirements that railroads and other hazardous materials transporters, as well as shippers, have and adhere to security plans.

FRA has an authorized inspection staff of about 400 persons nationwide, distributed across its eight regions. (In addition, about 160 inspectors employed by the 30

States that participate in FRA's State participation program inspect for compliance with FRA's standards.) The inspectors are experts in specific disciplines, including track, signal and train control, motive power and equipment, operating practices, and hazardous materials. In addition, we have 16 grade crossing experts in the field. Our inspectors conduct thousands of inspections every year, investigate more than 100 train accidents, investigate hundreds of complaints, develop recommendations for hundreds of enforcement actions, and engage in a range of educational activities on railroad safety issues. Although some inspectors have had basic familiarization training on security issues, they are not security experts.

The railroad industry's overall safety record has improved over the last decade, and most safety trends are moving in the right direction. However, significant train accidents continue to occur, and the train accident rate has not shown substantial improvement in recent years. Moreover, recent train accidents have highlighted specific issues that need prompt government and industry attention, and the strong growth of rail and highway traffic continues to drive up exposure at highway-rail grade crossings. FRA developed its Railroad Safety Action Plan to address these critical issues, and Secretary Mineta announced the plan in May 2005.

This Action Plan will:

- Target the most frequent, highest risk causes of accidents;
- Focus FRA's oversight and inspection resources; and
- Accelerate research efforts that have the potential to mitigate the largest risks.

FRA's plan includes initiatives in several areas: reducing human factor-caused train accidents; acting to address the serious problem of fatigue among railroad operating employees; improving track safety; enhancing hazardous materials safety and emergency preparedness; improving highway-rail grade crossing safety; and better focusing FRA's resources (inspections and enforcement) on areas of greatest safety concern. One of the primary elements of the Action Plan is FRA's implementation of its National Inspection Plan, which uses sophisticated trend analysis to ensure that FRA is properly allocating its inspectors within the regions so that they are directing their efforts toward the railroads that pose the highest risks. In addition, FRA has developed guidance for its inspectors in each discipline to help them use all available data to focus not only on the railroads with the highest risks but also on the particular kinds of noncompliance that involve the most significant hazards.

FRA has begun to move forward on all of the elements of its Action Plan, and has implemented its National Inspection Plan in the three areas that account for more than 75 percent of all train accidents: human factors; track; and equipment.

FRA's Role in Railroad Security

Since the terrorist attacks on September 11, 2001, FRA has been actively engaged in the railroad industry's response to the threat of terrorism. The railroads have developed their own security plans, and FRA has worked with the railroads, rail labor, and law enforcement personnel to develop the Railway Alert Network for the distribution of information and intelligence on security issues. Working with the Federal Transit Administration, another DOT agency, we have participated in security risk assessments on commuter railroads. FRA's security director works on a daily basis to facilitate communications on security issues between government agencies and the railroad industry.

In 2003, PHMSA (then the Research and Special Programs Administration) issued a rule requiring transporters and shippers of certain hazardous materials to develop and adhere to security plans. PHMSA issued its rule under its authority, delegated from the Secretary, to "prescribe regulations for the safe transportation, including security, of hazardous materials," 49 U.S.C. 5103(b)(1). Under the rule, security plans must include an assessment of security risks and appropriate measures to address those risks. The plans must, at a minimum, address three specific areas—personnel security, unauthorized access, and en route security. To assist railroads that transport hazardous materials and shippers that offer those materials for transport by rail, particularly small and medium-sized companies, to comply with this new requirement, FRA field personnel have spent a considerable amount of time in outreach efforts. To date, FRA personnel have reviewed more than 3,600 security plans and more than 29,000 employee security training records.

Since April 2004, FRA and PHMSA have also worked with DHS on a coordinated plan to improve the security of the rail transport of hazardous materials classified as toxic inhalation hazards (TIH). These include materials such as chlorine, which is used in water filtration plants, and anhydrous ammonia, which is used extensively in agriculture. DHS's Transportation Security Administration (TSA) has the lead on this project. TSA has led vulnerability assessments of a number of rail corridors where TIH materials are transported. DOT and TSA published a notice and request for comments in the *Federal Register* asking for input on aspects of TIH rail shipments, the DOT security program requirement, and the need for additional regulation, 69 Fed. Reg. 50988 (Aug. 16, 2004). More than 100 comments were received, addressing the following issues:

- security plan improvements;
- shipment identification and hazard communication;
- temporary storage;
- tank car integrity; and
- communication and tracking.

DOT is considering possible amendments to the PHMSA security plan rule that would enhance the security of the transportation of TIH materials.

In the area of passenger security, FRA inspectors have conducted basic security reviews of Amtrak and commuter railroad security both after the 2004 train bombings in Madrid and after the July 2005 transit bombings in London. In both cases, FRA inspectors were deployed immediately after the bombings to assess the security readiness of passenger railroad facilities based on a checklist of major security criteria. In the aftermath of the London bombings, FRA worked closely on these security reviews with TSA's new rail security inspectors. TSA focused primarily on urban rapid transit lines, while FRA inspectors concentrated on commuter and intercity passenger operations. In some situations, inspectors from the two agencies worked jointly.

FRA also supports research, development, and demonstration projects related to rail security through its Office of Research and Development (OR&D), often in cooperation with DHS. One completed project to evaluate tank car security and two current, follow-up projects provide examples. The tank car security evaluation project was conducted jointly by FRA OR&D and DHS in October 2003 at FRA's Transportation Technology Center, Inc., in Pueblo, Colorado. Its first purpose was to evaluate the ability of hydrophones inside tank cars to detect breaches and to distinguish noise coming from a breach of the tank car from other background noises such as those present in the normal tank car operating environment. Its second purpose was to develop emergency response techniques, tools, and procedures to plug punctures in pressurized tank cars caused by small arms fire or other means. A confidential report has been completed. The acoustic signatures of the small arms fire and other projectiles were recorded from both the hydrophones and accelerometers. The results of this test proved the feasibility of developing algorithms to monitor tank cars while under load. As a follow-on to this test, DHS and FRA funded an effort to look at the effects of small arms fire on tank cars and the use of hydrophones to sense a "hit." Development of the algorithm for detecting a hazardous material release event continues.

As a result of these tests, the Association of American Railroads (AAR) and contractors have examined various methods to "harden" tank cars. All of the options to "armor" tank cars available with today's technology are either too heavy or so expensive as to be economically impractical. FRA has learned about a new material, Dragon Shield, which is currently being used for armor coating military vehicles in Iraq. The Railway Supply Institute, the American Chemistry Council, the Chlorine Institute, and the AAR have worked with DHS and FRA in putting together a test plan to determine the feasibility of using this liquid armor (Dragon Shield) technology to reduce tank car vulnerability based upon the threat previously identified. Testing of the material will start in FY 2006. FRA's Office of Research and Development will continue to partner with DHS on these and other security initiatives.

In September 2004, DOT and DHS entered into a memorandum of understanding (MOU) concerning their respective roles on security issues. The MOU notes that DHS has the primary responsibility for security in all modes of transportation and that DOT plays a supporting role, but notes that both agencies have regulatory responsibilities in the area of transportation security. The MOU requires early coordination between the parties on the development of regulations affecting security. The MOU also contemplates the development of separate annexes on specific task and areas of responsibility. DOT and DHS have executed an annex concerning their joint project on the security of the transportation of TIH materials. FRA has also prepared a draft annex concerning rail security issues in general and has recently shared that draft with TSA. We hope to complete that annex soon.

FRA's Cooperation with TSA's New Inspection Force

The FY 2005 DHS Appropriations Bill Conference Report No. 108–774 earmarked $10 million for TSA to deploy up to 100 Federal rail security compliance inspectors. The first class of these inspectors completed training in early June 2005, and since then FRA has worked closely with the managers of TSA's new inspection program.

Through regular meetings and frequent contacts, we are developing working relationships at the headquarters and field levels of both agencies. We are trying to ensure that the two agencies' roles are clearly distinguished and do not result in duplicative inspections of the rail industry. As mentioned previously, inspectors from the two agencies have already engaged in a successful joint security review of passenger operations.

As TSA's full complement of inspectors becomes fully functional, FRA anticipates that there will be less need for FRA inspectors to participate in activities related purely to security. FRA's safety mission is critical and requires the constant attention of its inspection force. Of course, if FRA's inspectors are needed to support TSA's efforts for a limited duration in a time of an elevated security threat, FRA will make every effort to provide that support. Moreover, in those areas such as hazardous materials transportation where safety and security are significantly interrelated, FRA inspectors will continue to play an active role (e.g., in enforcing PHMSA's security plan regulations).

Conclusion

FRA's primary mission is helping to ensure the safety of railroad transportation. In some areas, such as hazardous materials transportation, safety and security are inextricably intertwined, which means that FRA's safety activities will no doubt continue to have an effect on security. In general, however, FRA's role is to support DHS and TSA in carrying out their security responsibilities, to the extent FRA can do so within its present authority and with its current resources.

The CHAIRMAN. Thank you very much. Ms. Berrick, Director of Homeland Security and Justice at GAO, please?

STATEMENT OF CATHLEEN A. BERRICK, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. BERRICK. Thank you, Mr. Chairman and Senator McCain, for the opportunity to discuss passenger rail security in the United States. My testimony today focuses on actions DHS has taken to assess the risk posed by terrorism to the rail system. Federal actions taken to enhance passenger rail security and security practices implemented by domestic and selected foreign passenger rail operators.

DHS, in conjunction with its grant-making authority, has completed numerous risk assessments of passenger rail systems around the country and has provided technical assistance and training to rail operators. The Department has also begun to develop an overall framework to help agencies in the private sector develop a consistent approach for analyzing and comparing risks to transportation and to other sectors.

TSA, as the lead agency responsible for securing all modes of transportation, has also begun to conduct risk assessments and establish a methodology for analyzing and characterizing risks. However, these efforts have not yet been completed or fully coordinated within the Federal Government and with rail operators. TSA has also missed deadlines in issuing its Transportation Sector Specific Plan, which is required by law and it's to identify and prioritize infrastructure protection efforts and key resources.

Until these efforts are completed, it may not be possible to compare risks within the rail sector and across different sectors, prioritize them and allocate resources accordingly.

After the 9/11 attacks, the Department of Transportation took several actions to strengthen rail security, including providing security training to rail operators and technical assistance in conducting risk assessments.

More recently, following the Madrid bombings, TSA issued emergency security directives to rail operators and pilot tested explosive detection technology for use in the rail system. However, some Federal and rail stake holders question the feasability of implementing and complying with these directives, claiming that they were not always based on industry best practices or were unclear. TSA also had not yet developed criteria or procedures for rail inspectors to use in enforcing compliance with the directives.

In response to a prior recommendation, DHS and DOT signed a Memorandum of Understanding last year, intended to improve coordination among Federal agencies and with rail stakeholders. And recently, in September of 2005, signed a transit security annex to this MOU. We are hopeful that this effort will increase coordination between the two departments and stakeholders to create a more unified and effective approach to securing rail.

We also found that domestic and foreign passenger rail operators have generally taken similar actions to secure their rail systems. For example, most have implemented customer awareness programs, to encourage passengers to report suspicious activities, increased the number and visibility of security personnel and upgraded their security technologies.

However, we also observe security practices among certain foreign rail operators or their governments that are not currently used or used to the same degree in the United States. These practices include the random screening of passengers and their bags, the utilization of covert testing to help keep employees alert to security threats, and building security into the design and refurbishing of rail stations. We also found that certain foreign governments maintain a clearinghouse of rail security technologies, which is not currently done in the U.S.

In conclusion, Mr. Chairman, we are encouraged by the steps DHS has taken to use elements of a risk management approach to guide infrastructure protection decisions for rail and across all sectors. However, we believe that enhanced Federal leadership is needed to help ensure that actions and investments designed to enhance security are properly focused and prioritized. Mr. Chairman, this concludes my opening statement. I'd be happy to respond to any questions at the appropriate time.

[The prepared statement of Ms. Berrick follows:]

PREPARED STATEMENT OF CATHLEEN A. BERRICK, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. Chairman and Members of the Committee:

Thank you for inviting me to participate in today's hearing on passenger and freight rail security. The London rail bombings that took place in July—resulting in over 50 fatalities and more than 700 injuries—made clear that even when a variety of security precautions are put in place, passenger rail systems that move high volumes of passengers on a daily basis remain vulnerable to terrorist attack. While securing the U.S. passenger rail system is a daunting task—a shared responsibility requiring coordinated action on the part of Federal, State, and local governments and the private sector—it is important nonetheless to take the necessary steps to identify and mitigate risks to passenger rail systems.

As we have reported previously, the sheer number of stakeholders involved in securing these systems can lead to communication challenges, duplication of effort, and confusion about roles and responsibilities. Key Federal stakeholders with critical roles to play within the rail sector include the Transportation Security Administration (TSA), which is responsible for transportation security overall, and the Office for Domestic Preparedness (ODP), which provides grant funds to rail operators and conducts risk assessments for passenger rail agencies, both within the Department of Homeland Security (DHS); and the Federal Transit Administration (FTA) and Federal Railroad Administration (FRA), both within the Department of Transportation (DOT). One of the critical challenges facing these Federal agencies, and rail system operators they oversee or support, is finding ways to protect rail systems from potential terrorist attacks without compromising the accessibility and efficiency of rail travel.

At the Federal level, another significant challenge to securing rail systems involves allocation of resources. The U.S. passenger rail systems represent one of many modes of transportation—along with aviation, maritime, and others—competing for limited Federal security resources. Within the passenger rail sector itself, there is competition for resources, as Federal, State, and local agencies and rail operators seek to identify and invest in appropriate security measures to safeguard these systems while also investing in other capital and operational improvements. Moreover, given competing priorities and limited homeland security resources, difficult policy decisions have to be made by Congress and the Executive Branch to prioritize security efforts and direct resources to areas of greatest risk within the passenger rail system, among all transportation modes, and across other nationally critical sectors.

In this regard, to help Federal decision makers determine how to best allocate limited resources, we have advocated, the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) has recommended, and the subsequent Intelligence Reform and Terrorism Prevention Act of 2004 requires, that a risk management approach be employed to guide security decision making. [1] A risk management approach entails a continuous process of managing risks through a series of actions, including setting strategic goals and objectives, assessing and quantifying risks, evaluating alternative security measures, selecting which measures to undertake, and implementing and monitoring those measures. In July 2005, in announcing his proposal for the reorganization of DHS, the Secretary of DHS declared that as a core principle of the reorganization, the Department must base its work on priorities driven by risk.

My testimony today focuses on the progress Federal agencies and domestic passenger rail operators have made in setting and implementing security priorities in the wake of September 11 and terrorist attacks on rail systems, and the security practices implemented by foreign passenger rail operators. In particular, my testimony highlights three key areas: (1) the actions that DHS and its component agencies have taken to assess the risks posed by terrorism to the U.S. passenger rail system in the context of prevailing risk management principles; (2) the actions that Federal agencies have taken to enhance the security of the U.S. passenger rail system; and (3) the security practices that domestic and selected foreign passenger rail operators have implemented to mitigate risks and enhance security, and any differences in these practices. My comments today are based upon our recently issued report to Senators Snowe and Boxer of this Committee, the Chairman of the House Transportation and Infrastructure Subcommittee on Railroads, and Representative Castle. [2]

In summary:

- Within DHS, ODP has completed numerous risk assessments of passenger rail systems around the country, and TSA has begun to conduct risk assessments as well as establish a methodology for determining how to analyze and characterize risks that have been identified. Until TSA completes these efforts, however, or sets timelines for doing so, the agency will not be able to prioritize passenger rail assets and help guide security investment decisions. At the department level, DHS has begun developing, but has not yet completed a framework to help agencies and the private sector develop a consistent approach for analyzing and comparing risks to transportation and other sectors. Until this framework is finalized and shared with stakeholders, it may not be possible to compare risks across different sectors, prioritize them, and allocate resources accordingly.
- In addition to the ongoing initiatives to enhance passenger rail conducted by the FTA and FRA, in 2004, TSA issued emergency security directives to domestic rail operators after terrorist attacks on the rail system in Madrid and piloted a test of explosive detection technology for use in passenger rail systems. However, Federal and rail industry officials raised questions about the feasibility of implementing and complying with these directives, citing limited opportunities to collaborate with TSA to ensure that industry best practices were incorporated. In September 2004, DHS and DOT signed a memorandum of under-

standing to improve coordination between the two agencies, and are developing agreements to delineate specific security-related roles and responsibilities, among other things, for the different modes. An agreement for transit security was signed in September 2005.

- Domestic and foreign passenger rail operators we contacted have taken a range of actions to help secure their systems. Most, for example, had implemented customer awareness programs to encourage passengers to remain vigilant and report suspicious activities, increased the number and visibility of their security personnel, increased the use of canine teams to detect explosives, enhanced employee training programs, upgraded security technology, tightened access controls, and made rail system design improvements to enhance security. We also observed security practices among certain foreign passenger rail systems or their governments that are not currently used by the domestic rail operators we contacted, or by the U.S. Government, which could be considered for use in the United States. For example, some foreign rail operators randomly screen passengers or utilize covert testing to help keep employees alert to security threats, and some foreign governments maintain centralized clearinghouses on rail security technologies and best practices. While introducing any of these security practices into the U.S. rail system may pose political, legal, fiscal, and cultural challenges, they may nevertheless warrant further examination.

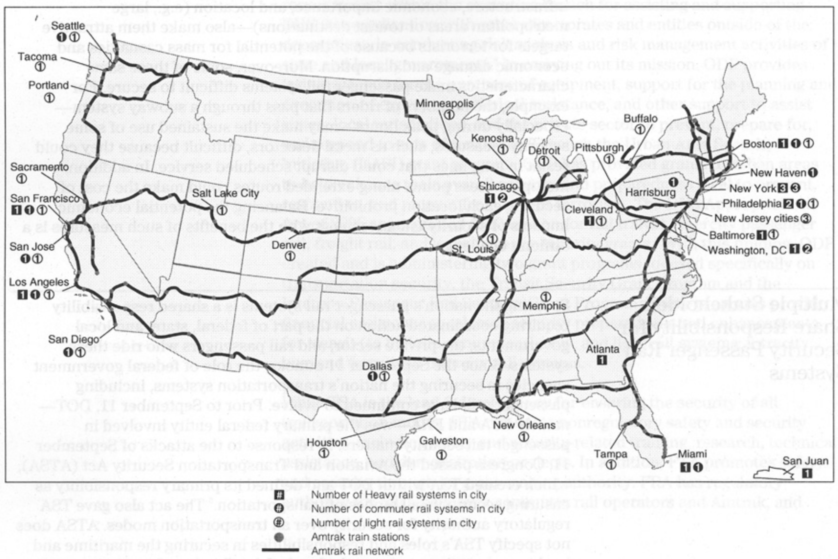
In our September 2005 report on passenger rail security, we recommended, among other things, that to help ensure that the Federal Government has the information it needs to prioritize passenger rail assets based on risk, and in order to evaluate, select, and implement commensurate measures to help the Nation's passenger rail operators protect their systems against acts of terrorism, TSA should establish a plan with timelines for completing its methodology for conducting risk assessments and develop security standards that reflect industry best practices and can be measured and enforced, by using the Federal rule-making process. In addition, we recommended that the Secretary of DHS, in collaboration with DOT and the passenger rail industry, determine the feasibility, in a risk management context, of implementing certain security practices used by foreign rail operators. DHS, DOT, and Amtrak generally agreed with the report's recommendations.

Background

Overview of the Passenger Rail System

Each weekday, 11.3 million passengers in 35 metropolitan areas and 22 states use some form of rail transit (commuter, heavy, or light rail).[3] Commuter rail systems typically operate on railroad tracks and provide regional service (e.g., between a central city and adjacent suburbs). Commuter rail systems are traditionally associated with older industrial cities, such as Boston, New York, Philadelphia, and Chicago. Heavy rail systems—subway systems like New York City's transit system and Washington, D.C.'s Metro—typically operate on fixed rail lines within a metropolitan area and have the capacity for a heavy volume of traffic. Amtrak operates the Nation's primary intercity passenger rail service over a 22,000-mile network, primarily over leased freight railroad tracks.[4] Amtrak serves more than 500 stations (240 of which are staffed) in 46 states and the District of Columbia, and it carried more than 25 million passengers in 2004. Figure 1 identifies the geographic location of rail transit systems and Amtrak within the United States.

Figure 1: Geographic Distribution of Amtrak and Rail Transit Systems



Source: Amtrak and National Transit Database.

Passenger Rail Systems Are Inherently Vulnerable to Terrorist Attacks

According to passenger rail officials and passenger rail experts, certain characteristics of domestic and foreign passenger rail systems make them inherently vulnerable to terrorist attacks and therefore difficult to secure. By design, passenger rail systems are open (i.e., have multiple access points, hubs serving multiple carriers, and, in some cases, no barriers) so that they can move large numbers of people quickly. In contrast, the U.S. commercial aviation system is housed in closed and controlled locations with few entry points. The openness of passenger rail systems can leave them vulnerable because operator personnel cannot completely monitor or control who enters or leaves the systems. In addition, other characteristics of some passenger rail systems—high ridership, expensive infrastructure, economic importance, and location (e.g., large metropolitan areas or tourist destinations)—also make them attractive targets for terrorists because of the potential for mass casualties and economic damage and disruption. Moreover, some of these same characteristics make passenger rail systems difficult to secure. For example, the numbers of riders that pass through a subway system—especially during peak hours—may make the sustained use of some security measures, such as metal detectors, difficult because they could result in long lines that could disrupt scheduled service. In addition, multiple access points along extended routes could make the cost of securing each location prohibitive. Balancing the potential economic impacts of security enhancements with the benefits of such measures is a difficult challenge.

Multiple Stakeholders Share Responsibility for Security Passenger Rail Systems

Securing the Nation's passenger rail systems is a shared responsibility requiring coordinated action on the part of Federal, State, and local governments; the private sector; and rail passengers who ride these systems. Since the September 11 attacks, the role of Federal Government agencies in securing the Nation's transportation systems, including passenger rail, have continued to evolve. Prior to September 11, DOT—namely FTA and FRA—was the primary Federal entity involved in passenger rail security matters. In response to the attacks of 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. [5] The Act also gave TSA regulatory authority for security over all transportation modes. ATSA does not specify TSA's roles and responsibilities in securing the maritime and land transportation modes at the level of detail it does for aviation security. Instead, the Act broadly identifies that TSA is responsible for ensuring the security of all modes of transportation. With the passage of the Homeland Security Act of 2002, TSA was transferred, along with over 20 other agencies, to the Department of Homeland Security.[6]

With the creation of DHS in 2002, one of its components, ODP, became primarily responsible for overseeing security funding for passenger rail systems.[7] ODP is the principal component of DHS responsible for preparing the United States for acts of terrorism and has primary responsibility within the executive branch for assisting and supporting DHS, in coordination with other directorates and entities outside of the Department, in conducting risk analysis and risk management activities of state and local governments.[8] In carrying out its mission, ODP provides training, funds for the purchase of equipment, support for the planning and execution of exercises, technical assistance, and other support to assist states, local jurisdictions, and the private sector to prevent, prepare for, and respond to acts of terrorism. Through the Urban Area Security Initiative (UASI) grant program, ODP has provided grants to urban areas to help enhance their overall security and preparedness level to prevent, respond to, and recover from acts of terrorism. The DHS Appropriations Act of 2005 appropriated $150 million for rail transit, intercity passenger rail, freight rail, and transit agency security grants.[9] With this funding, ODP created and is administering two grant programs focused specifically on transportation security, the Transit Security Grant Program and the Intercity Passenger Rail Security Grant Program. These programs provide financial assistance to address security preparedness and enhancements for transit (to include commuter, heavy, and light rail systems; intracity bus; and ferry) and intercity rail systems.

While TSA is the lead Federal agency for ensuring the security of all transportation modes, FTA conducts nonregulatory safety and security activities, including safety and security-related training, research, technical assistance, and demonstration projects. In addition, FTA promotes safety and security through its grant-making authority. FRA has regulatory authority for rail safety over commuter rail operators and Amtrak, and employs over 400 rail inspectors that periodically monitor the implementation of safety and security plans at these systems.[10]

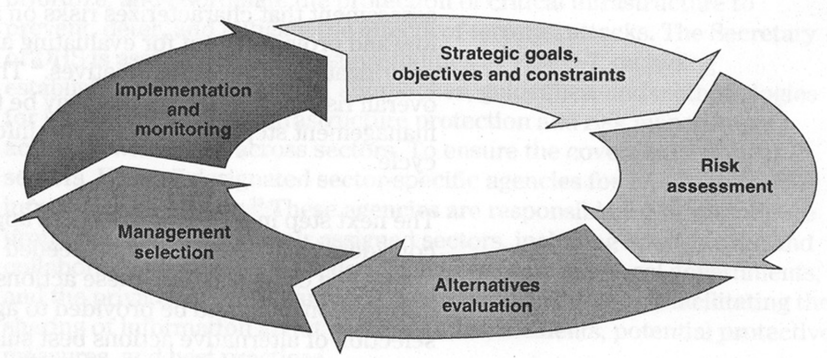
State and local governments, passenger rail operators, and private industry are also important stakeholders in the Nation's rail security efforts. State and local governments may own or operate a significant portion of the passenger rail system. Even when state and local governments are not owners and operators, they are directly affected by passenger rail systems that run within and through their jurisdictions. Consequently, the responsibility for responding to emergencies involving the passenger rail infrastructure often falls to state and local governments. Passenger rail operators, which can be public or private entities, are responsible for administering and managing passenger rail activities and services. Passenger rail operators can directly operate the service provided or contract for all or part of the total service. Although all levels of government are involved in passenger rail security, the primary responsibility for securing passenger rail systems rests with the passenger rail operators.

Assessing and Managing Risks to Rail Infrastructure Using a Risk Management Approach

In recent years, we, along with Congress (most recently through the Intelligence Reform and Terrorism Prevention Act of 2004),[11] the executive branch (e.g., in presidential directives), and the 9/11 Commission have required or advocated that Federal agencies with homeland security responsibilities utilize a risk management approach to help ensure that finite national resources are dedicated to assets or activities considered to have the highest security priority. We have concluded that without a risk management approach, there is limited assurance that programs designed to combat terrorism are properly prioritized and focused. Thus, risk management, as applied in the homeland security context, can help to more effectively and efficiently prepare defenses against acts of terrorism and other threats.

A risk management approach entails a continuous process of managing risk through a series of actions, including setting strategic goals and objectives, performing risk assessments, evaluating alternative actions to reduce identified risks by preventing or mitigating their impact, management selecting actions to undertake, and implementing and monitoring those actions. Figure 2 depicts a risk management cycle that is our synthesis of government requirements and prevailing best practices previously reported.

Figure 2: Risk Management Cycle



Source: GAO.

Setting strategic goals, objectives, and constraints is a key first step in implementing a risk management approach and helps to ensure that management decisions are focused on achieving a strategic purpose. These decisions should take place in the context of an agency's strategic plan that includes goals and objectives that are clear, concise, and measurable.

Risk assessment, a critical element of a risk management approach, helps decision makers identify and evaluate potential risks so that countermeasures can be designed and implemented to prevent or mitigate the effects of the risks. 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. Risk assessment in a homeland security application often involves assessing three key elements—threat, criticality, and vulnerability:

- A threat assessment identifies and evaluates potential threats on the basis of factors such as capabilities, intentions, and past activities.
- A criticality or consequence assessment evaluates and prioritizes assets and functions in terms of specific criteria, such as their importance to public safety and the economy, as a basis for identifying which structures or processes are relatively more important to protect from attack.
- A vulnerability assessment identifies weaknesses that may be exploited by identified threats and suggests options to address those weaknesses.

Information from these three assessments contributes to an overall risk assessment that characterizes risks on a scale such as high, medium, or low and provides input for evaluating alternatives and management prioritization of security initiatives.[12] The risk assessment element in the overall risk management cycle may be the largest change from standard management steps and is central to informing the remaining steps of the cycle.

The next step in a risk management approach—alternatives evaluation—considers what actions may be needed to address identified risks, the associated costs of taking these actions, and any resulting benefits. This information is then to be provided to agency management to assist in the selection of alternative actions best suited to the unique needs of the organization. An additional step in the risk management approach is the implementation and monitoring of actions taken to address the risks, including evaluating the extent to which risk was mitigated by these actions. Once the agency has implemented the actions to address risks, it should develop criteria for and continually monitor the performance of these actions to ensure that they are effective and also reflect evolving risk.

Federal Agencies with Risk Management Responsibilities

A number of Federal departments and agencies have risk management and critical infrastructure protection responsibilities stemming from various requirements. The Homeland Security Act of 2002, which created DHS, directed the Department's Information Analysis and Infrastructure Protection (IAIP) Directorate to utilize a risk management approach in coordinating the Nation's critical infrastructure protection efforts. This includes using risk assessments to set priorities for protective and support measures by the Department, other Federal agencies, State and local government agencies and authorities, the private sector, and other entities. Homeland Security Presidential Directive 7 (HSPD–7) defines critical infrastructure protection responsibilities for DHS, sector-specific agencies (those Federal agencies given responsibility for transportation, energy, telecommunications, and so forth), and other departments and agencies. The President instructs Federal departments and agencies to identify, prioritize, and coordinate the protection of critical infrastructure to prevent, deter, and mitigate the effects of terrorist attacks. The Secretary of DHS is assigned several responsibilities by HSPD–7, including establishing uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors. To ensure the coverage of critical sectors, HSPD–7 designated sector-specific agencies for 17 critical infrastructure sectors. [13] These agencies are responsible for infrastructure protection activities in their assigned sectors, including coordinating and collaborating with relevant Federal agencies, state and local governments, and the private sector to carry out their responsibilities and facilitating the sharing of information about vulnerabilities, incidents, potential protective measures, and best practices.

Pursuant to HSPD–7 and the National Infrastructure Protection Plan (NIPP), DHS was designated as the sector-specific agency for the transportation sector, a responsibility the Department has delegated to TSA. [14] As the sector-specific agency for transportation, TSA is required to develop a transportation sector-specific plan (TSSP) for identifying, prioritizing, and protecting critical transportation infrastructure and key resources that will provide key input to the broader National Infrastructure Protection Plan to be prepared by IAIP. DHS issued an interim NIPP in February 2005 that was intended to serve as a road map for how DHS and stakeholders—including other Federal agencies, the private sector, and state and local governments—should use risk management principles for determining how to prioritize activities related to protecting critical infrastructure and key resources within and among each of the 17 sectors in an integrated, coordinated fashion. DHS expects the next iteration of the NIPP to be issued in November 2005, with the sector-specific plans, including the TSSP, being incorporated into this plan in February 2006. HSPD–7 also requires DHS to coordinate with DOT on all transportation security matters.

DHS Has Taken Steps to Assess Risk to Passenger Rail Systems, but Additional Work Is Needed to Guide Security Investments

DHS component agencies have taken various steps to assess the risk posed by terrorism to U.S. passenger rail systems. ODP has developed and implemented a risk assessment methodology intended to help passenger rail operators and others enhance their capacity to respond to terrorist incidents and identify and prioritize security countermeasures. As of July 2005, ODP had completed 7 risk assessments with rail operators and 12 others were under way. Further, TSA completed a threat assessment for mass transit and rail and has begun to identify critical rail assets, but it has not yet completed an overall risk assessment for the passenger rail industry. DHS is developing guidance to help these and other sector-specific agencies work with stakeholders to identify and analyze risk.

ODP Has Worked with Passenger Rail Operators to Develop Risk Assessments to Help Prioritize Rail Security Needs and Investments

In 2002, ODP began conducting risk assessments of passenger rail operators through its Mass Transit Technical Assistance program. These assessments are intended to help passenger rail operators and port authorities enhance their capacity and preparedness to respond to terrorist incidents involving weapons of mass destruction, and identify and prioritize security countermeasures and emergency response capabilities. ODP's approach to risk assessment is generally consistent with the risk assessment component of our risk management approach. The agency has worked with passenger rail operators and others to complete several risk assessments. As of July 2005, ODP had completed 7 risk assessments in collaboration with passenger rail operators. [15] Twelve additional risk assessments are under way, and an additional 11 passenger rail operators have requested assistance through this program. The results developed in the threat, criticality, vulnerability, and impact assessments are then used to develop an overall risk assessment in order to evaluate the relative risk among various assets, weapons, and modes of attack. This is intended to give operators an indication of which asset types and threat scenarios carry the highest risk that, accordingly, are likely candidates for early risk mitigation action.

According to rail operators who have used ODP's risk assessment methodology and commented about it to DHS or us, the method has been successful in helping to devise risk reduction strategies to guide security-related investments. For example, between September 2002 and March 2003, ODP's technical assistance team worked with the Port Authority of New York and New Jersey (PANYNJ) to conduct a risk assessment of all of its assets—its Port Authority Trans-Hudson (PATH) passenger rail system, as well as airports, ports, interstate highway crossings, and commercial properties.[16] According to PANYNJ officials, the authority was able to develop and implement a risk reduction strategy that enabled it to identify and set priorities for improvements in security and emergency response capability that are being used to guide security investments. According to authority officials, the risk assessment that was conducted was instrumental in obtaining management approval for a 5-year, $500 million security capital investment program, as it provided a risk-based justification for these investments.

The six other passenger rail operators that have completed ODP's risk assessment process also stated that they valued the process. Specifically, operators said that the assessments enabled them to prioritize investments based on risk and are already allowing or are expected to allow them to effectively target and allocate resources toward security measures that will have the greatest impact on reducing risk across their system.

ODP Has Sought to Promote Risk-Based Decision Making Among Federal Agencies and Rail Operators

On the basis of its own experience with conducting risk assessments in the field, and in keeping with its mission to develop and implement a national program to enhance the capacity of state and local agencies to respond to incidents of terrorism, ODP has offered to help other DHS components and Federal agencies to develop risk assessment tools, according to ODP officials. For example, ODP is partnering with FRA, TSA, the American Association of Railroads (AAR), and others to develop a risk assessment tool for freight rail corridors.[17] In a separate Federal outreach effort, ODP worked with TSA to establish a Federal Risk Assessment Working Group to promote interagency collaboration and information sharing. In addition, in keeping with its mission to deliver technical assistance and training, ODP has partnered with the American Public Transportation Association (APTA) to inform passenger rail operators about its risk assessment technical assistance program.[18] Since June 2004, ODP has attended five APTA conferences or workshops where it has set up information booths, made the tool kit available, and conducted seminars to educate passenger rail operators about the risk assessment process and its benefits.

ODP has leveraged its grant-making authority to promote risk-based funding decisions for passenger rail. For example, passenger rail operators must have completed a risk assessment to be eligible for financial assistance through the Fiscal Year 2005 Transit Security Grant Program administered by ODP. To receive these funds, passenger rail operators are also required to have a security and emergency preparedness plan that identifies how the operator intends to respond to security gaps identified by risk assessments. This plan, along with a regional transit security strategy prepared by regional transit stakeholders, will serve as the basis for determining how the grant funds are to be allocated.

Risk assessments are also a key driver of Federal funds distributed through ODP's Fiscal Year 2005 Intercity Passenger Rail Grant Program. This $7.1 million program provides financial assistance to Amtrak for the protection of critical infrastructure and emergency preparedness activities along Amtrak's Northeast Corridor and its hub in Chicago. Amtrak is required to conduct a risk assessment of these areas in collaboration with ODP, in order to receive the grant funds.[19] A recent review of Amtrak's security posture and programs conducted by the RAND Corporation and funded by FRA in 2004 found that no comprehensive terrorism risk assessment of Amtrak has been conducted that would provide an empirical baseline for investment prioritization and decision making for Amtrak's security policies and investment plans. As another condition for receiving the grant funds, Amtrak is required to develop a security and emergency preparedness plan that, along with the risk assessment, is to serve as the basis for proposed allocations of grant funding. According to an Amtrak security official, it welcomes the risk assessment effort and plans to use the results of the assessment to guide its security plans and investments. According to ODP officials, as of July 2005, the Amtrak risk assessment was nearly 50 percent complete.

TSA Has Begun to Assess Risks to Passenger Rail

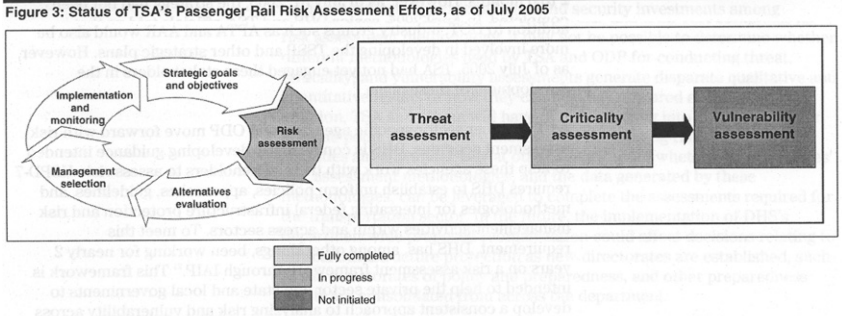
In October 2004, TSA completed an overall threat assessment for both mass transit and passenger and freight rail modes.[20] TSA began conducting a second risk assessment element—criticality assessments of passenger rail stations—in the spring of 2004, but the effort had not been completed at the time of our review. According to TSA, a criticality assessment tool was developed that considers multiple factors, such as the potential for loss of life or effects on public health; the economic impact of the loss of function of the asset and the cost of reconstitution; and the local, regional, or national symbolic importance of the asset. These factors were to be used to arrive at a criticality score that, in turn, would enable the agency to rank assets and facilities based on relative importance, according to TSA officials.

To date, TSA has assigned criticality scores to nearly 700 passenger rail stations. In May 2005, TSA began conducting assessments for other passenger rail assets such as bridges and tunnels. TSA officials told us that as of July 2005, they had completed 73 criticality assessments for bridge and tunnel assets and expect to conduct approximately 370 additional assessments in these categories. Once TSA has completed its criticality assessment, a senior group of transportation security experts will review these scores and subsequently rank and prioritize them. As of July 2005, TSA had not established a time frame for completing criticality assessments for passenger rail assets or for ranking assets, and had not identified whether it planned to do so.

In 2003, TSA officials stated that they planned to work with transportation stakeholders to rank assets and facilities in terms of their criticality. HSPD–7 requires sector-specific agencies such as TSA to collaborate with all relevant stakeholders, including Federal departments and agencies, state and local governments, and others. In addition, DHS's interim NIPP states that sector-specific agencies, such as TSA, are expected to work with stakeholders—such as rail operators—to determine the most effective means of obtaining and analyzing information on assets. While TSA's methodology for conducting criticality assessments calls for "facilitated sessions" involving TSA modal specialists, DOT modal specialists, and trade association representatives, these sessions with stakeholders have not been held. According to TSA officials, their final methodology for conducting criticality assessments did not include DOT modal specialists and trade associations. With respect to rail operators, TSA officials explained that their risk assessment process does not require operators' involvement. TSA analysts said they have access to a great deal of information (such as open source records, satellite imagery, and insurance industry data) that can facilitate the assessment process. However, when asked to comment on TSA's ability to identify critical assets in passenger rail systems, APTA officials and 10 rail operators we interviewed told us it would be difficult for TSA to complete this task without their direct input and rail system expertise.

TSA plans to rely on asset criticality rankings to prioritize which assets it will focus on in conducting vulnerability assessments. That is, once an asset, such as a passenger rail station, is deemed to be most critical, then TSA would focus on determining the station's vulnerability to attacks. TSA plans to conduct on-site vulnerability assessments for those assets deemed most critical. For assets that are deemed to be less critical, TSA has developed a software tool that it has made available to passenger rail and other transportation operators for them to use on a voluntary basis to assess the vulnerability of their assets. As of July 2005, the tool had not yet been used. According to APTA officials, passenger rail operators may be reluctant to provide vulnerability information to TSA without knowing how the agency intends to use such information. According to TSA, it is difficult, if not impossible, to project any timelines regarding completion of vulnerability assessments in the transportation sector because rail operators are not required to submit them. In this regard, while the rail operators are not required to submit this information, as the sector-specific agency for transportation, TSA is required by HSPD–7 to complete vulnerability assessments for the transportation sector. Figure 3 illustrates the overall progress TSA had made in conducting risk assessments for passenger rail assets as of July 2005.

Figure 3: Status of TSA's Passenger Rail Risk Assessment Efforts, as of July 2005



Source: GAO.

We recognize that TSA's risk assessment effort is still evolving and TSA has had other pressing priorities, such as meeting the legislative requirements related to aviation security. However, until all three assessments of rail systems—threat, criticality, and vulnerability—have been completed in sequence, and until TSA determines how to use the results of these assessments to analyze and characterize risk (e.g., whether high, medium, or low), it may not be possible to prioritize passenger rail assets and guide investment decisions about protecting them.

Finalizing a methodology for assessing risk to passenger rail and other transportation assets and conducting the assessments are key steps needed to produce the plans required by HSPD–7 and the Intelligence Reform and Terrorism Prevention Act of 2004. DHS and TSA have missed both deadlines for producing these plans. Specifically, DHS and TSA have not yet produced the TSSP required by HSPD–7 to be issued in December of 2004, though a draft was prepared in November 2004. DHS and TSA also missed the April 1, 2005, deadline for completing the national strategy for transportation security required by the Intelligence Reform and Terrorism Prevention Act of 2004. In an April 2005 letter to Congress addressing the missed deadline, the DHS Deputy Secretary identified the need to more aggressively coordinate the development of the strategy with other relevant planning work such as the TSSP, to include further collaboration with DOT modal administrations and DHS components. The Deputy Secretary further stated that DHS expected to finish the strategy within 2 to 3 months. However, as of July 31, 2005, the strategy had not been completed. In April 2005, senior DHS and TSA officials told us that in addition to DOT, industry groups such as APTA and AAR would also be more involved in developing the TSSP and other strategic plans. However, as of July 2005, TSA had not yet engaged these stakeholders in the development of these plans.

As TSA, other sector-specific agencies, and ODP move forward with risk assessment activities, DHS is concurrently developing guidance intended to help these agencies work with their stakeholders to assess risk. HSPD–7 requires DHS to establish uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors. To meet this requirement, DHS has, among other things, been working for nearly 2 years on a risk assessment framework through IAIP.[21] This framework is intended to help the private sector and state and local governments to develop a consistent approach to analyzing risk and vulnerability across infrastructure types and across entire economic sectors, develop consistent terminology, and foster consistent results. The framework is also intended to enable a Federal-level assessment of risk in general, and comparisons among risks, for purposes of resource allocation and response planning. DHS has informed TSA that this framework will provide overarching guidance to sector-specific agencies on how various risk assessment methodologies may be used to analyze, normalize, and prioritize risk within and among sectors. The interim NIPP states that the ability to rationalize, or normalize, results of different risk assessments is an important goal for determining risk-related priorities and guiding investments. One core element of the DHS framework—defining concepts, terminology, and metrics for assessing risk—had not yet been completed. The completion date for this element—initially due in September 2004—has been extended twice, with the latest due date in June 2005. However, as of July 31, 2005, this element has not been completed.

Because neither this element nor the framework as a whole has been finalized or provided to TSA or other sector-specific agencies, it is not clear what impact, if any, DHS's framework may have on ongoing risk assessments conducted by, and the methodologies used by, TSA, ODP, and others, and whether or how DHS will be able to use these results to compare risks and prioritize homeland security investments among sectors. Until DHS finalizes this framework, and until TSA completes its risk assessment methodology, it may not be possible to determine whether different methodologies used by TSA and ODP for conducting threat, criticality, and vulnerability assessments generate disparate qualitative and quantitative results or how they can best be compared and analyzed. In addition, TSA and others will have difficulty taking into account whether at some point TSA may be unnecessarily duplicating risk management activities already under way at other agencies and whether other agencies' risk assessment methodologies, and the data generated by these methodologies, can be leveraged to complete the assessments required for the transportation sector. In the future, the implementation of DHS's department-wide proposed reorganization could affect decisions relating to critical infrastructure protection as new directorates are established, such as the directorates of policy and preparedness, and other preparedness assets are consolidated from across the department.

Multiple Federal Agencies Have Taken Actions to Enhance Passenger Rail Security

FTA and FRA were the primary Federal agencies involved in passenger rail security matters prior to the creation of TSA. Before and after September 11, these two agencies launched a number of initiatives designed to strengthen passenger rail security. TSA also took steps to strengthen rail security, including issuing emergency security directives to rail operators and testing emerging rail security technologies for screening passengers and baggage. Rail industry stakeholders and Federal agency officials raised questions about how effectively DHS had collaborated with them on rail security issues. DHS and DOT have signed a memorandum of understanding intended to identify ways that collaboration with Federal and industry stakeholders might be improved.

DOT Agencies Led Initial Efforts to Enhance Passenger Rail Security

Prior to the creation of TSA in November 2001, DOT agencies (i.e., modal administrations)—notably FTA and FRA—were primarily responsible for the security of passenger rail systems. These agencies undertook a number of initiatives to enhance the security of passenger rail systems after September 11. FTA, using an $18.7 million appropriation by the Department of Defense and Emergency Supplemental Appropriations Act of 2002, launched a multipart transit security initiative, much of which is still in place. The initiative included security readiness assessments, technical assistance, grants for emergency response drills, and training. For example, in 2003, FTA instituted the Transit Watch campaign—a nationwide safety and security awareness program designed to encourage the active participation of transit passengers and employees in maintaining a safe transit environment. The program provides information and instructions to transit passengers and employees so that they know what to do and whom to contact in the event of an emergency in a transit setting. FTA plans to continue this initiative, in partnership with TSA and ODP, and offer additional security awareness materials that address unattended bags and emergency evacuation procedures for transit agencies. In addition, FTA has issued guidance, such as its Top 20 Security Program Action Items for Transit Agencies, which recommends measures for passenger rail operators to implement into their security programs to improve both security and emergency preparedness.

FTA has also used research and development funds to develop guidance for security design strategies to reduce the vulnerability of transit systems to acts of terrorism. In November 2004, FTA provided rail operators with security considerations for transportation infrastructure. This guidance provided recommendations intended to help operators deter and minimize attacks against their facilities, riders, and employees by incorporating security features into the design of rail infrastructure.

FRA has also taken a number of actions to enhance passenger rail security since September 11. For example, it has assisted commuter railroads in developing security plans, reviewed Amtrak's security plans, and helped fund FTA security readiness assessments for commuter railroads. More recently, in the wake of the Madrid terrorist bombings, nearly 200 FRA inspectors, in cooperation with DHS, conducted multi-day team inspections of each of the 18 commuter railroads and Amtrak to determine what additional security measures had been put into place to prevent a similar occurrence in the United States. FRA also conducted research and development projects related to passenger rail security. These projects included rail infrastructure security and trespasser monitoring systems and passenger screening and manifest projects, including explosives detection.

Although DOT modal administrations now play a supporting role in transportation security matters since the creation of TSA, they remain important partners in the Federal Government's efforts to improve rail security, given their role in funding and regulating the safety of passenger rail systems. Moreover, as TSA moves ahead with its passenger rail security initiatives, FTA and FRA are continuing their passenger rail security efforts.

TSA Issued Mandatory Security Directives to Rail Operators but Faces Challenges Related to Compliance and Enforcement

In response to the March 2004 commuter rail attacks in Madrid and Federal intelligence on potential threats against U.S. passenger rail systems, TSA issued security directives to the passenger rail industry in May 2004. TSA issued these security directives to establish a consistent baseline standard of protective measures for all passenger rail operators, including Amtrak.[22] The directives were not related to, and were issued independent of, TSA's efforts to conduct risk assessments to prioritize rail security needs. TSA considered the measures required by the directives to constitute mandatory security standards that were required to be implemented within 72 hours of issuance by all passenger rail operators nationwide. In an effort to provide some flexibility to the industry, the directives allowed rail operators to propose alternative measures to TSA in order to meet the required measures. Table 1 contains examples of security measures required by these directives.

TABLE 1: EXAMPLES OF MEASURES REQUIRED BY TSA SECURITY DIRECTIVES ISSUED TO PASSENGER RAIL OPERATORS AND AMTRAK

TSA directives require passenger rail operators to:

- designate coordinators to enhance security-related communications with TSA;
- provide TSA with access to the latest security assessments and security plans;
- reinforce employee watch programs;
- ask passengers and employees to report unattended property or suspicious behavior;
- remove trash receptacles at stations determined by a vulnerability assessment to be at significant risk and only to the extent practical, except for clear plastic or bomb-resistant containers;
- install bomb-resistant trash cans to the extent resources allow;
- utilize canine explosive detection teams, if available, to screen passenger baggage, terminals, and trains;
- utilize surveillance systems to monitor for suspicious activity, to the extent resources allow;
- allow TSA-designated canine teams at any time or place to conduct canine operations;
- conduct frequent inspections of key facilities, stations, terminals, or other critical assets for persons and items that do not belong;
- inspect each passenger rail car for suspicious or unattended items, at regular periodic intervals;
- ensure that appropriate levels of policing and security are provided that correlate to DHS threat levels and threat advisories;
- lock all doors that allow access to train operators' cab or compartment, if equipped with locking mechanisms;
- require Amtrak to request that adult passengers provide identification at the initial point where tickets are checked.

Source: TSA.

Although TSA issued these directives, it is unclear how TSA developed the required measures contained in the directives, how TSA plans to monitor and ensure compliance with the measures, how rail operators are to implement the measures, and which entities are responsible for their implementation. According to the former DHS Undersecretary for Border and Transportation Security, the directives were developed based upon consultation with the industry and a review of best practices in passenger rail and mass transit systems across the country and were intended to provide a Federal baseline standard for security. TSA officials stated to us that the directives were based upon FTA and APTA best practices for rail security. Specifically, TSA stated that it consulted a list of the top 20 actions FTA identified that rail operators can take to strengthen security, FTA-recommended protective measures and activities for transit agencies that may be followed based on current threat levels, and an APTA member survey. While some of the directives correlate to information contained in the FTA guidance, such as advocating that rail personnel watch for abandoned parcels, vehicles, and the like, the source for many of the directives is unclear. For example, the source material TSA consulted does not support the requirement that train cabs or compartment doors should be kept locked. Furthermore, the sources do not necessarily reflect industry best practices, according to FTA and APTA officials. FTA's list of recommended protective measures and the practices identified in the APTA survey are not necessarily viewed as industry best practices. For example, the APTA member survey that TSA used reports rail security practices that are in use by operators but which are not best practices endorsed by the group or other industry stakeholders.

TSA officials have stated that they understood the importance of partnering with the rail industry on security matters, and that they would draw on the expertise and knowledge of the transportation industry and other DHS agencies, as well as all stakeholders, in developing security standards for all modes of transportation, including rail. TSA officials held an initial meeting with APTA, AAR, and Amtrak officials to discuss the draft directives prior to their issuance and told them that they would continue to be consulted prior to their final issuance. However, these stakeholders were not given an opportunity to comment on a final draft of the directives before their release because, according to TSA, DHS determined that it was important to release the directives as soon as possible to address a current threat to passenger rail. In addition, TSA stated that because the directives needed to be issued quickly, there was no public comment as part of the rule-making process. Shortly after the directives were issued, TSA's Deputy Assistant Administrator for Maritime and Land Security told rail operators at an APTA conference we attended in June 2004 that if TSA determined that there is a need for the directives to become permanent, they would undergo a notice-and-comment period as part of the regulatory process. As of July 2005, TSA had not yet determined whether it intends to pursue the rule-making process with a notice and comment period.

APTA and AAR officials stated that because they were not consulted throughout the development of the directives, the directives did not, in their view, reflect a complete understanding of the passenger rail environment or necessarily incorporate industry best practices. For example, APTA, AAR, and some rail operators raised concerns about the feasibility of installing bomb-resistant trash cans in rail stations because they could direct the force of a bomb blast upward, possibly causing structural damage in underground or enclosed stations. DHS's Office for State and Local Government Coordination and Preparedness recently conducted tests to determine the safety and effectiveness of 13 models of commercially available bomb-resistant trash receptacles. At the time of our review, the results of these tests were not yet available.

Amtrak and FRA officials raised concerns about some of the directives, as well, and told us they questioned whether the requirements reflected industry best practices. For example, before the directives were issued, Amtrak expressed concerns to TSA about the feasibility of the requirement to check the identification of all adult passengers boarding its trains because it did not have enough staff to perform these checks. However, the final directive included this requirement, and after they were released, Amtrak told TSA it could not comply with this requirement "without incurring substantial additional costs and significant detrimental impacts to its operations and revenues." Amtrak officials told us that since passenger names would not be compared against any criminal or terrorist watch list or database, the benefits of requiring such identification checks were open to debate. To resolve its concern, and as allowed by the directive, Amtrak proposed, and TSA accepted, random identification checks of passengers as an alternative measure. FRA officials further stated that current FRA safety regulations requiring engineer compartment doors be kept unlocked to facilitate emergency escapes[23] conflicts with the security directive requirement that doors equipped with locking mechanisms be kept locked. This requirement was not included in the draft directives provided to stakeholders. TSA did call one commuter rail operator prior to issuing the directives to discuss this potential proposed measure, and the operator raised a concern about the safety of the locked door requirement. TSA nevertheless included this requirement in the directives.

With respect to how the directives were to be enforced, rail operators were required to allow TSA and DHS to perform inspections, evaluations, or tests based on execution of the directives at any time or location. Upon learning of any instance of noncompliance with TSA security measures, rail operators were to immediately initiate corrective action. Monitoring and ensuring compliance with the directives has posed challenges for TSA. In the year after the directives were issued, TSA did not have dedicated field staff to conduct on-site inspections. When the rail security directives were issued, the former DHS Undersecretary for Border and Transportation Security stated that TSA planned to form security partnership teams with DOT, including FRA rail inspectors, to help ensure that industry stakeholders complied with the directives. These teams were to be established in order to tap into existing capabilities and avoid duplication of effort across agencies. As of July 2005, these teams had not yet been utilized to perform inspections. TSA has, however, hired rail compliance inspectors to, among other things, monitor and enforce compliance with the security directives. As of July 2005, TSA had hired 57 of up to 100 inspector positions authorized by Congress.[24] However, TSA has not yet established processes or criteria for determining and enforcing compliance, including determining how rail inspectors or DOT partnership teams will be used in this regard.

Establishing criteria for monitoring compliance with the directives may be challenging because the language describing the required measures allows for flexibility and does not define parameters. In an effort to acknowledge the variable conditions that existed in passenger rail environments, TSA designed the directives to allow flexibility in implementation through the use of such phrases as “to the extent resources allow,” “to the extent practicable,” and “if available.” The directives also include nonspecific instructions that may be difficult to measure or monitor, telling operators to, for example, perform inspections of key facilities at “regular periodic intervals” or to conduct “frequent inspections” of passenger rail cars. When the directives were issued, TSA stated that it would provide rail operators with performance-based guidance and examples of announcements and signs that could be used to meet the requirements of the directives, including guidance on the appropriate frequency and method for inspecting rail cars and facilities. However, as of July 2005, this information had not been provided.

Industry stakeholders we interviewed raised questions about how they were to comply with the measures contained in the directives and which entities were responsible for implementing the measures. According to an AAR official, in June 2004, AAR officials and rail operators held a conference call with TSA to obtain clarification on these issues. According to AAR officials, in response to an inquiry about what would constitute compliance for some of the measures, the then-TSA Assistant Administrator for Maritime and Land Security told participants that the directives were not intended to be overly prescriptive but were guidelines, and that operators would have the flexibility to implement the directives as they saw fit. The officials also asked for clarification on who was legally responsible for ensuring compliance for measures where assets, such as rail stations, were owned by freight railroads or private real estate companies. According to AAR officials, TSA told them it was the responsibility of the rail operators and asset owners to work together to determine these responsibilities. However, according to AAR and rail operators, given that TSA has hired rail inspectors and indicated its intention to enforce compliance with the directives, it is critical that TSA clarify what compliance entails for measures required by the directives and which entities are responsible for compliance with measures when rail assets are owned by one party but operated by another—such as when private companies that own terminals or stations provide services for commuter rail operations.

The challenges TSA has faced in developing security directives as standards that reflect industry best practices—and that can be measured and enforced—stem from the original emergency nature of the directives, which were issued with limited input and review. TSA told rail industry stakeholders when the directives were issued 15 months ago that the agency would consider using the Federal rule-making process as a means of making the standards permanent. Doing so would require TSA to hold a notice-and-comment period, resulting in a public record that reflects stakeholders’ input on the applicability and feasibility of implementing the directives, along with TSA’s rationale for accepting or rejecting this input. While there is no guarantee that this process would produce more effective security directives, it would be more transparent and could help TSA in developing standards that are most appropriate for the industry and can be measured, monitored, and enforced.

TSA Has Begun Testing Rail Security Technologies

In addition to issuing security directives, TSA also sought to enhance passenger rail security by conducting research on technologies related to screening passengers and checked baggage in the passenger rail environment. Beginning in May 2004, TSA conducted a Transit and Rail Inspection Pilot (TRIP) study, in partnership with DOT, Amtrak, the Connecticut Department of Transportation, the Maryland Transit Administration, and the Washington Metropolitan Area Transit Authority (WMATA). TRIP was a $1.5 million, three-phase effort to test the feasibility of using existing and emerging technologies to screen passengers, carry-on items, checked baggage, cargo, and parcels for explosives. Figure 4 summarizes TRIP's three-phased approach.

Figure 4: Summary Information on TSA's Transit and Rail Inspection Pilot Program Phases

Phase I: Screen commuter rail passengers and carry-on baggage before trains are boarded using an explosive detection device similar in appearance to an airport metal detector and other explosive screening technologies.

Phase II: Screen passenger baggage including checked baggage, unclaimed baggage, and cargo on long-haul Amtrak trains prior to departure.

Phase III: Screen passengers and their carry-on baggage on board a moving commuter rail train. All passengers are required to enter the train in the specially designed screening car, which was a commuter rail passenger car that been reconfigured to hold screening equipment and security personnel.

Source: TSA.

According to TSA, all three phases of the TRIP program were completed by July 2004. However, TSA has not yet issued a planned report analyzing whether the technologies could be used effectively to screen rail passengers and their baggage. According to TSA officials, a report on results and lessons learned from TRIP is under review by DHS. TSA officials told us that based upon preliminary analyses, the screening technologies and processes tested would be very difficult to implement on more heavily used passenger rail systems because these systems carry high volumes of passengers and have multiple points of entry. However, TSA officials stated to us that the screening processes used in TRIP may be useful on certain long-distance intercity train routes, which make fewer stops. Further, officials stated that screening could be used either randomly or for all passengers during certain high-risk events or in areas where a particular terrorist threat is known to exist. For example, screening technology similar to that used in TRIP was used by TSA to screen certain passengers and belongings in Boston and New York during the Democratic and Republican national conventions, respectively, in 2004.

APTA officials and the 28 passenger rail operators we interviewed—all who are not directly involved in the pilot—agreed with TSA's preliminary assessment. They told us they believed that the TRIP screening procedures could not work in most passenger rail systems, given the number of passengers using these systems and the open nature (e.g., multiple entry points) of the systems. For example, as one operator noted, over 1,600 people pass through dozens of access points in New York's Penn Station per minute during a typical rush hour, making screening of all passengers very challenging, if not impossible. Passenger rail operators were also concerned that screening delays could result in passengers opting to use other modes of transportation. APTA officials and some rail operators we interviewed said that had they been consulted by TSA, they would have recommended alternative technologies to explore and indicated that they hoped to be consulted on security technology pilot programs in the future. FRA officials further stated that TSA could have benefited from earlier and more frequent collaboration with them during the TRIP pilot than occurred, and could have tapped their expertise to analyze TRIP results and develop the final report. TSA research and development officials told us that the agency has begun to consider and test security technologies other than those used in TRIP, which may be more applicable to the passenger rail environment. For example, TSA's and DHS's Science and Technology Directorate are currently evaluating infrared cameras and electronic metal detectors, among other things.

DHS and DOT Are Taking Steps to Improve Coordination and Collaboration With Federal Agencies and Industry Stakeholders

In response to a previous recommendation we made in a June 2003 report on transportation security, DHS and DOT signed a memorandum of understanding (MOU) to develop procedures by which the two departments could improve their cooperation and coordination for promoting the safe, secure, and efficient movement of people and goods throughout the transportation system. The MOU defines broad areas of responsibility for each department. For example, it states that DHS, in consultation with DOT and affected stakeholders, will identify, prioritize, and coordinate the protection of critical infrastructure. The MOU between DHS and DOT represents an overall framework for cooperation that is to be supplemented by additional signed agreements, or annexes, between the departments. These annexes are to delineate the specific security-related roles, responsibilities, resources, and commitments for mass transit, rail, research and development, and other matters. The annex for mass transit security was signed in September 2005.[25] According to DHS and DOT officials, this annex is intended to ensure that the programs and protocols for incorporating stakeholder feedback and making enhancements to security measures are coordinated. For example, the annex requires that DHS and DOT consult on such matters as regulations and security directives that affect security and identifies points of contact for coordinating this consultation.

In addition to their work on the MOU and related annexes, DHS and TSA have taken other steps in an attempt to improve collaboration with DOT and industry stakeholders. In April 2005, DHS officials stated that better collaboration with DOT and industry stakeholders was needed to develop strategic security plans associated with various homeland security presidential directives and statutory mandates, such as the Intelligence Reform and Terrorism Prevention Act of 2004, which required DHS to develop a national strategy for transportation security in conjunction with DOT. Responding to the need for better collaboration, DHS established a senior-level steering committee in conjunction with DOT to coordinate development of this national strategy. In addition, senior DHS and TSA officials stated that industry groups will also be involved in developing the national strategy for transportation security and other strategic plans. Moreover, according to TSA's assistant administrator for intermodal programs, TSA intends to work with APTA and other industry stakeholders in developing security standards for the passenger rail industry.[26]

U.S. and Foreign Rail Operators Have Taken Similar Actions to Secure Rail Systems, and Opportunities for Additional Domestic Security Actions May Exist

U.S. passenger rail operators have taken numerous actions to secure their rail systems since the terrorist attacks of September 11 in the United States, and the March 11, 2004, attacks in Madrid. These actions included both improvements to system operations and capital enhancements to a system's facilities, such as track, buildings, and train cars. All of the U.S. passenger rail operators we contacted have implemented some types of security measures—such as increased numbers and visibility of security personnel and customer awareness programs—that were generally consistent with those we observed in select countries in Europe and Asia. We also identified three rail security practices—covert testing, random screening of passengers and their baggage, and centralized research and testing—utilized by foreign operators or their governments that are not currently utilized by domestic rail operators or the U.S. government.[27]

Actions Taken by U.S. and Foreign Passenger Rail Operators to Strengthen Security Reflect Security Assessments, Budgetary Constraints, and Other Factors

All 32 of the U.S. rail operators we interviewed or visited reported taking specific actions to improve the security and safety of their rail systems by, among other things, investing in new security equipment, utilizing more law enforcement personnel, and establishing public awareness campaigns. Passenger rail operators we spoke with cited the 1995 sarin gas attacks on the Tokyo subway system and the September 11 terrorist attacks as catalysts for their security actions. After the attacks, many passenger rail operators used FTA's security readiness assessments of heavy and passenger rail systems as a guide to determine how to prioritize their security efforts, as well as their own understanding of their system's vulnerabilities, to determine what actions to take to enhance security. Similarly, as previously mentioned, the rail systems that underwent ODP risk assessments are currently using or plan to use these assessments to guide their security actions. In addition, 20 of the 32 U.S. operators we contacted or visited had conducted some type of security assessment internally or through a contractor, separate from the federally funded assessments. For example, some assessments evaluated vulnerabilities of physical assets, such as tunnels and bridges, throughout the passenger rail system. Passenger rail operators stated that security-related spending by rail operators was also based, in part, on budgetary considerations, as well as other practices used by other rail operators that were identified through direct contact or during industry association meetings.[28] Passenger rail operators frequently made capital investments to improve security, and these investments often are not part of Federal funding packages for new construction unless they are part of new facilities being constructed. According to APTA, 54 percent of transit agencies are facing increasing deficits, and no operator covers expenses with fare revenue; thus, balancing operational and capital improvements with security-related investments has been an ongoing challenge for these operators. Several foreign rail operators we interviewed also stated that funding for security enhancements was limited in light of other funding priorities within the rail system, such as personnel costs and infrastructure and equipment maintenance.

Foreign rail operators we visited also told us that risk assessments played an important role in guiding security-related spending for rail. For example, one foreign rail operator with a daily ridership of 2.3 million passengers used a risk management methodology to assess risks, threats, and vulnerabilities to rail in order to guide security spending. The methodology is part of the rail operator's corporate focus on overall safety and security and is intended to help protect the operator's various rail systems against, among other things, terrorist attacks, as well as other forms of corporate loss, such as service disruption and loss of business viability.

U.S. and Foreign Rail Operators Employ Similar Security Practices

Both U.S. and foreign passenger rail operators we contacted have implemented similar improvements to enhance the security of their systems. [29] A summary of these efforts follows.

Customer awareness: Customer awareness programs we observed used signage and announcements to encourage riders to alert train staff if they observed suspicious packages, persons, or behavior. Of the 32 domestic rail operators we interviewed, 30 had implemented a customer awareness program or made enhancements to an existing program. Foreign rail operators we visited also attempt to enhance customer awareness. For example, 11 of the 13 operators we interviewed had implemented a customer awareness program. Similar to programs of U.S. operators, these programs used signage, announcements, and brochures to inform passengers and employees about the need to remain vigilant and report any suspicious activities. Only one of the European passenger rail operators that we interviewed has not implemented a customer security awareness program, citing the fear or panic that it might cause among the public.

Increased number and visibility of security personnel: Of the 32 U.S. rail operators we interviewed, 23 had increased the number of security personnel they utilized since September 11 to provide security throughout their system or had taken steps to increase the visibility of their security personnel. In addition to adding security personnel, many operators stated that increasing the visibility of security was as important as increasing the number of personnel. For example, several U.S. and foreign rail operators we spoke with had instituted policies such as requiring their security staff, in brightly colored vests, to patrol trains or stations more frequently, so they are more visible to customers and potential terrorists or criminals. These policies make it easier for customers to contact security personnel in the event of an emergency, or if they have spotted a suspicious item or person. At foreign sites we visited, 10 of the 13 operators had increased the number of their security officers throughout their systems in recent years because of the perceived increase in risk of a terrorist attack.

Increased use of canine teams: Of the 32 U.S. passenger rail operators we contacted, 21 had begun to use canine units, which include both dogs and human handlers, to patrol their facilities or trains or had increased their existing utilization of such teams. Often, these units are used to detect the presence of explosives, and may be called in when a suspicious package is detected. Some operators that did not maintain their own canine units stated that it was prohibitively expensive to do so and that they could call in local police canine units if necessary. In foreign countries we visited, passenger rail operators' use of canines varied. In some Asian countries, canines were not culturally accepted by the public and thus were not used for rail security purposes. As in the United States, and in contrast to Asia, most European passenger rail operators used canines for explosive detection or as deterrents.

Employee training: All of the domestic and foreign rail operators we interviewed had provided some type of security training to their staff, either through inhouse personnel or an external provider. In many cases, this training consisted of ways to identify suspicious items and persons and how to respond to events once they occur. For example, the London Underground and the British Transport Police developed the "HOT" method for its employees to identify suspicious items in the rail system. In the HOT method, employees are trained to look for packages or items that are Hidden, Obviously suspicious, and not Typical of the environment. Items that do not meet these criteria would likely receive a lower security response than an item meeting all of the criteria. However, if items meet all of these criteria, employees are to notify station managers, who would call in the authorities and potentially shut down the station or take other action. According to London Underground officials, the HOT method has significantly reduced the number of system disruptions caused when a suspicious item was identified. Several passenger rail operators in the United States and abroad have trained their employees in the HOT method. Several domestic operators had also trained their employees in how to respond to terrorist attacks and provided them with wallet-size cards highlighting actions they should take in response to various forms of attack. It is important to note that training such as the HOT method is not designed to prevent acts of terrorism like the July 2005 London attacks, where suicide bombers killed themselves rather than leaving bombs behind.

Passenger and baggage screening practices: Some domestic and foreign rail operators have trained employees to recognize suspicious behavior as a means of screening passengers. Eight U.S. passenger rail operators we contacted were utilizing some form of behavioral screening. For example, the Massachusetts Bay Transportation Authority (MBTA), which operates Boston's T system, has utilized a behavioral screening system to identify passengers exhibiting suspicious behavior. The Massachusetts State Police train all MBTA personnel to be on the lookout for behavior that may indicate someone has criminal intent, and to approach and search such persons and their baggage when appropriate. Massachusetts State Police officers have been training rail operators on this behavior profiling system, and WMATA and New Jersey Transit were among the first additional operators to implement the system. According to MBTA personnel, several other operators have expressed interest in this system. Abroad, we found that 4 of 13 operators we interviewed had implemented forms of behavioral screening similar to MBTA's system.

All of the domestic and foreign rail operators we contacted have ruled out an airport-style screening system for daily use in heavy traffic, where each passenger and the passenger's baggage are screened by a magnetometer or X-ray machine, based on cost, staffing, and customer convenience factors, among others. For example, although the Spanish National Railway screens passenger baggage using an X-ray machine on certain long-distance trains that it believes could be at risk, all of the operators we contacted stated that the cost, staffing requirements, delay of service, and inconvenience to passengers would make such a system unworkable in highly trafficked, inherently open systems like U.S. and foreign passenger rail operations. In addition, one Asian rail official stated that his organization was developing a contingency plan for implementing an airport-style screening system, but that such a system would be used only in the event of intelligence information indicating suicide bomb attacks were imminent, or if several attacks had already occurred during a short period of time. According to this official, the plan was in the initial stages of development, and the organization did not know how quickly such a system could be implemented.

Upgrading technology: Many rail operators we interviewed had embarked on programs designed to upgrade their existing security technology. For example, we found that 29 of the 32 U.S. operators had implemented a form of CCTV to monitor their stations, yards, or trains. While these cameras cannot be monitored closely at all times, because of the large number of staff they said this would require, many rail operators felt the cameras acted as a deterrent, assisted security personnel in determining how to respond to incidents that have already occurred, and could be monitored if an operator has received information that an incident may occur at a certain time or place in their system. One rail operator, New Jersey Transit, had installed "smart" cameras, which were programmed to alert security personnel when suspicious activity occurred, such as if a passenger left a bag in a certain location or if a boat were to dock under a bridge. According to the New Jersey Transit officials, this technology was relatively inexpensive and not difficult to implement. Several other operators stated they were interested in exploring this technology. Abroad, all 13 of the foreign rail operators we visited had CCTV systems in place. As in the United States, foreign rail operators use these cameras primarily as a crime deterrent and to respond to incidents after they occur, because they do not have enough staff to continuously monitor all of these cameras.

In addition, 18 of the 32 U.S. rail operators we interviewed had installed new emergency phones or enhanced the visibility of the intercom systems they already had. Passengers can use these systems to contact train operators or security personnel to report suspicious activity, crimes in progress, or other problems. Furthermore, while most rail operators we spoke with had not installed chemical or biological agent detection equipment because of the costs involved, a few operators had this equipment or were exploring purchasing it. For example, WMATA, in Washington, D.C., has installed these sensors in some of its stations, thanks to a program jointly sponsored by DOT and the Department of Energy that provided this equipment to WMATA because of the high perceived likelihood of an attack in Washington, D.C. Also, at least three other domestic rail operators we spoke with are exploring the possibility of partnering with Federal agencies to install such equipment in their facilities on an experimental basis.

Also, as in the United States, a few foreign operators had implemented chemical or biological detection devices at these rail stations, but their use was not widespread. Two of the 13 foreign operators we interviewed had implemented these sensors, and both were doing so on an experimental basis. In addition, police officers from the British Transport Police—responsible for policing the rail system in the United Kingdom—were equipped with pagers to detect chemical, biological, or radiological elements in the air, allowing them to respond quickly in case of a terrorist attack using one of these methods. The British Transit Police also has three vehicles carrying devices to determine if unattended baggage contains explosives—these vehicles patrol the system 24 hours per day.

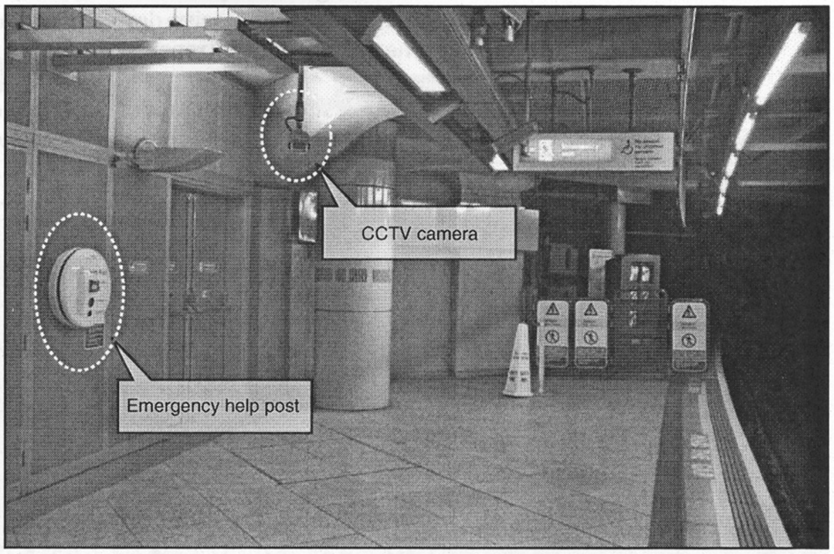
Access control: Tightening access procedures at key facilities or rights-of-way is another way many rail operators have attempted to enhance security. A majority of domestic and selected foreign passenger rail operators had invested in enhanced systems to control unauthorized access at employee facilities and stations. Specifically, 23 of the 32 U.S. operators had installed a form of access control at key facilities and stations. This often involved installing a system where employees had to swipe an access card to gain access to control rooms, repair facilities, and other key locations. All 13 foreign operators had implemented some form of access control to their critical facilities or rights-of-way. These measures varied from simple alarms on doors at electrical substations on one subway system we visited to infrared sensors monitoring every inch of right-of-way along the track on three of the high-speed interurban rail systems.

Rail system design and configuration: In an effort to reduce vulnerabilities to terrorist attack and increase overall security, passenger rail operators in the United States and abroad have been, or are now beginning to, incorporate security features into the design of new and existing rail infrastructure, primarily rail stations. For example, of the 32 domestic rail operators we contacted, 22 of them had removed their conventional trash bins entirely, or replaced them with transparent or bomb-resistant trash bins, as TSA instructed in its May 2004 security directives. Foreign rail operators had taken steps to remove traditional trash bins from their systems. Of the 13 operators we visited, 8 had either removed their trash bins entirely or replaced them with blast-resistant cans or transparent receptacles.

Many foreign rail operators are also incorporating aspects of security into the design of their rail infrastructure. Of the 13 operators we visited, 11 have attempted to design new facilities with security in mind and have attempted to retrofit older facilities to incorporate security-related modifications. For example, one foreign operator we visited is retrofitting its train cars with windows that passengers could open in the event of a chemical attack. In addition, the London Underground, one of the oldest rail systems in the world, incorporates security into the design of all its new stations as well as when existing stations are modified. We observed several security features in the design of Underground stations, such as using vending machines that have no holes that someone could use to hide a bomb, and sloped tops to reduce the likelihood that a bomb can be placed on top of the machine. In addition, stations are designed to provide staff with clear lines of sight to all areas of the station, such as underneath benches or ticket machines, and station designers try to eliminate or restrict access to any recessed areas where a bomb could be hidden.

In one London station, we observed the use of netting throughout the station to help prevent objects, such as bombs, from being placed in a recessed area, such as beneath a stairwell or escalator. In this station and other stations we visited, Underground officials have installed "help posts" at which customers can call for help if an incident occurs. When these posts are activated, CCTV cameras display a video image of the help post and surrounding area to staff at a central command center. This allows the staff to directly observe the situation and respond appropriately. See figure 5 for a photograph of a help post.

Figure 5: Security Design Elements Incorporated into London's Underground



Source: London Underground.

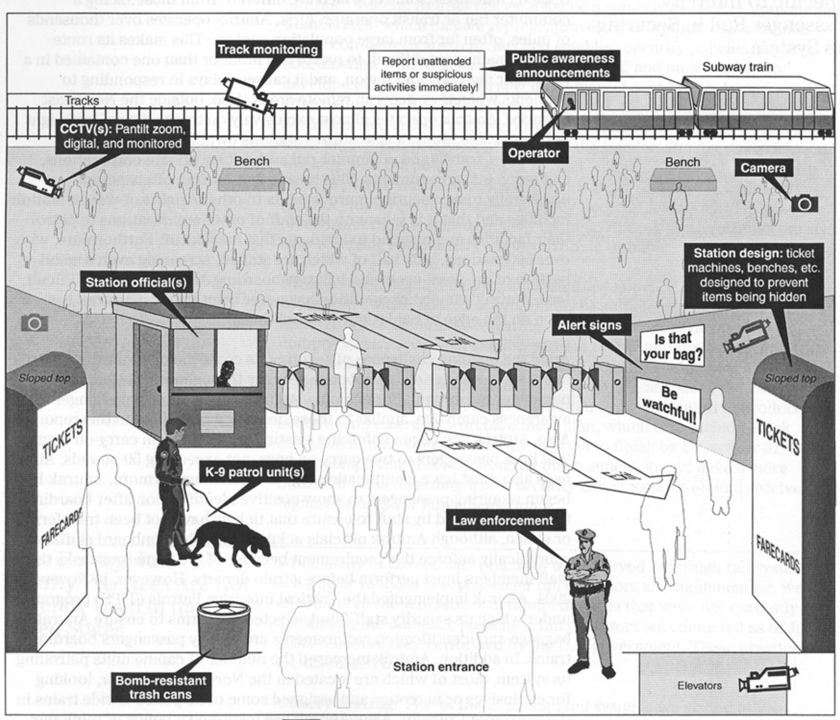
The "help post" in this London Underground rail station allows passengers to contact station security staff in an emergency. Once activated, the CCTV camera would be turned on so security staff could monitor the situation and identify what actions to take.

Underground officials stated that the incorporation of security features in station design is an effective measure in deterring some terrorists from attacking the system. For example, officials told us that CCTV video recorded the efforts by Irish Republican Army terrorists attempting to place an explosive device inside a station—and when they could not find a suitable location to hide the device, they placed it outside in a trash can instead, thereby mitigating the impact of the explosion.

In the United States, several passenger rail operators stated that they were taking security into account when designing new facilities or remodeling older ones. Twenty-two of 32 rail operators we interviewed told us that they were incorporating security into the design of new or existing rail infrastructure. For example, New York City Transit and PATH officials told us they are incorporating security into the design of its new stations, including the redesigned Fulton Street station and the World Trade Center Hub that were damaged or destroyed during the September 11 attacks. In addition, in June 2005, FTA issued guidelines for use by the transit industry encouraging the incorporation of particular security features into the design of transit infrastructure. These guidelines include, for example, increasing visibility for onboard staff, reducing the areas where someone could hide an explosive device on a transit vehicle, and enhancing emergency exits in transit stations.

Figure 6 shows a diagram of several security measures that we observed in passenger rail stations both in the United States and abroad. It should be noted that this represents an amalgam of stations we visited, not any particular station.

Figure 6: Composite of Selected Security Practices in the Passenger Rail Environment



Security resources currently used

Source: GAO and NOVA Development Corporation.

Amtrak Faces Challenges Specific to Intercity Passenger Rail in Securing Its System

In securing its extensive system, Amtrak faces its own set of security-related challenges, some of which are different from those facing a commuter rail or transit operator. First, Amtrak operates over thousands of miles, often far from large population centers. This makes its route system much more difficult to patrol and monitor than one contained in a particular metropolitan region, and it causes delays in responding to incidents when they occur in remote areas. Also, outside the Northeast Corridor, Amtrak operates almost exclusively on tracks owned by freight rail companies. Amtrak also utilizes stations owned by freight rail companies, transit and commuter rail authorities, private corporations, and municipal governments. This means that Amtrak often cannot unilaterally make security improvements to others' rights-of-way or station facilities and that it is reliant on the staff of other organizations to patrol their facilities and respond to incidents that may occur. Furthermore, with over 500 stations, only half of which are staffed, screening even a small portion of the passengers and baggage boarding Amtrak trains is difficult. Last, Amtrak's financial condition has never been strong—Amtrak has been on the edge of bankruptcy several times.

Amid the ongoing challenges of securing its coast-to-coast railway, Amtrak has taken some actions to enhance security throughout its intercity passenger rail system. For example, Amtrak has initiated a passenger awareness campaign, similar to those described elsewhere in this report. Also, Amtrak has begun enforcing existing restrictions on carry-on luggage that limit passengers to two carry-on bags, not exceeding 50 pounds. All bags also must have identification tags on them. Furthermore, Amtrak has begun requiring passengers to show positive identification after boarding trains when asked by staff to ensure that tickets have not been transferred or stolen, although Amtrak officials acknowledge their onboard staffs only sporadically enforce this requirement because of the numerous tasks these staff members must perform before a train departs. However, in November 2004, Amtrak implemented the Tactical Intensive Patrols (TIPS) program, under which its security staff flood selected platforms to ensure Amtrak baggage and identification requirements are met by passengers boarding trains. In addition, Amtrak increased the number of canine units patrolling its system, most of which are located in the Northeast Corridor, looking for explosives or narcotics and assigned some of its police to ride trains in the Northeast Corridor. Also, Amtrak has instituted a policy of randomly inspecting checked luggage on its trains. Finally, Amtrak is making improvements to the emergency exits in certain tunnels to make evacuating trains in the tunnels easier in the event of a crash or terrorist attack.

To ensure that security measures are applied consistently throughout Amtrak's system, Amtrak has established a series of Security Coordinating Committees, which include representatives of all Amtrak departments. These committees are to review and establish security policies, in coordination with Amtrak's police department, and have worked to develop countermeasures to specific threats. According to Amtrak, in the aftermath of the July 2005 London bombings, these committees met with Amtrak police and security staff to ensure additional security measures were implemented. Also in the wake of the London attacks, Amtrak began working with the police forces of several large east coast cities, allowing them to patrol Amtrak stations to provide extra security. In addition, all Amtrak employees now receive a "Daily Security Awareness Tip" and are receiving computer-based security training. Amtrak police officers are also now receiving specialized counter-terrorism training.

While Amtrak has taken the actions outlined above, it is difficult to determine if these actions appropriately or sufficiently addressed pressing security needs. As discussed earlier, Amtrak has not performed a comprehensive terrorism risk assessment that would provide an empirical baseline for investment prioritization and decision making for Amtrak's security policies and investment plans. However, as part of the 2005 Intercity Passenger Rail Grant Program, Amtrak is required to produce a security and emergency preparedness plan, which is to include a risk assessment that Amtrak currently expects to finish by December 31, 2005. Upon completing this plan, Amtrak management should have a more informed basis regarding which security enhancements should receive the highest priority for implementation.

Three Foreign Rail Security Practices Are Not Currently Used in the United States

While many of the security practices we observed in foreign rail systems are similar to those U.S. passenger rail operators are implementing, we encountered three practices in other countries that were not currently in use among the domestic passenger rail operators we contacted as of June 2005, nor were they performed by the U.S. Government. These practices are discussed below.

Covert testing: Two of the 13 foreign rail systems we visited utilize covert testing to keep employees alert about their security responsibilities. Covert testing involves security staff staging unannounced events to test the response of railroad staff to incidents such as suspicious packages or setting off alarms. In one European system, this covert testing involves security staff placing suspicious items throughout their system to see how long it takes operating staff to respond to the item. Similarly, one Asian rail operator's security staff will break security seals on fire extinguishers and open alarmed emergency doors randomly to see how long it takes staff to respond. Officials of these operators stated that these tests are carried out on a daily basis and are beneficial because their staff know they could be tested at any moment, and they, therefore, are more likely to be vigilant with respect to security.

Random screening: Of the 13 foreign operators we interviewed, 2 have some form of random screening of passengers and their baggage in place. In the systems where this is in place, security personnel can approach passengers either in stations or on the trains and ask them to submit their persons or their baggage to a search. Passengers declining to cooperate must leave the system. For example, in Singapore, rail agency officials rotate the stations where they conduct random searches so that the searches are carried out at a different station each day. Prior to the July 2005 London bombings, no passenger rail operators in the United States were practicing a form of random passenger or baggage screening on a continuing daily basis. However, during the Democratic National Convention in 2004, MBTA instituted a system of random screening of passengers, where every 11th passenger at certain stations and times of the day was asked to provide his or her bags to be screened. Those who refused were not allowed to ride the system. MBTA officials recognized that it is impossible to implement such a system comprehensively throughout the rail network without massive amounts of additional staff, and that even doing random screening on a regular basis would be a drain on resources. However, officials stated that such a system is workable during special events and times of heightened security but would have to be designed very carefully to ensure that passengers' civil liberties were not violated. After the July 2005 London bombings, four passenger rail operators—PATH, New York Metropolitan Transportation Authority, New Jersey Transit, and Utah Transit Authority in Salt Lake City—implemented limited forms of random bag screening in their system. In addition, APTA, FTA, and the National Academy of Science's Transportation Research Board are currently conducting a study on the benefits and challenges that passenger rail operators would face in implementing a randomized passenger screening system. The study is examining such issues as the legal basis for conducting passenger screening or search, the precedence for such measures in the transportation environment, the human resources required, and the financial implications and cost considerations involved.

National government maintains clearinghouse on technologies and best practices: According to passenger rail operators in five countries we visited, their national governments have centralized the process for performing research and developing passenger rail security technologies and maintaining a clearinghouse on these technologies and security best practices. According to these officials, this allows rail operators to have one central source for information on the merits of a particular passenger rail security technology, such as chemical sensors, CCTVs, and intrusion detection devices. Some U.S. rail operators we interviewed expressed interest in there being a more active centralized Federal research and development authority in the United States to evaluate and certify passenger rail security technologies and make that information available to rail operators. Although TSA is the primary Federal agency responsible for conducting transportation security research and development, and has conducted the TRIP as previously mentioned, most of the agency's research and development efforts to date have focused on aviation security technologies. As a result, domestic rail operators told us that they rely on consultations with industry trade associations, such as APTA, to learn about best practices for passenger rail security technologies and related investments. Several rail operators stated that they were often unsure of where to turn when seeking information on security-related products, such as CCTV cameras or intrusion detection systems. Currently, many operators said they informally ask other rail operators about their experiences with a certain technology, perform their own research via the Internet or trade publications, or perform their own testing.

No Federal agency has compiled or disseminated best practices to rail operators to aid in this process. We have previously reported that stakeholders have stated that the Federal Government should play a greater role in testing transportation security technology and making this information available to industry stakeholders.[30] TSA and DOT agree that making the results of research testing available to industry stakeholders could be a valuable use of Federal resources by reducing the need for multiple rail operators to perform the same research and development efforts, but they have not taken action to address this.[31]

Implementing these three practices—covert testing, random screening, and a government-sponsored clearinghouse for technologies and best practices—in the United States could pose political, legal, fiscal, and cultural challenges because of the differences between the United States and these foreign nations. For instance, many foreign nations have dealt with terrorist attacks on their public transportation systems for decades, compared with the United States, where rail transportation has not been specifically targeted during terrorist attacks. According to foreign rail operators, these experiences have resulted in greater acceptance of certain security practices, such as random searches, which the U.S. public may view as a violation of their civil liberties or which may discourage them from using public transportation. The impact of security measures on passengers is an important consideration for domestic rail transit operators, since most passengers could choose another means of transportation, such as a personal automobile. As such, security measures that limit accessibility, cause delays, increase fares, or otherwise cause inconvenience could push people away from transit and into their cars. In contrast, the citizens of the European and Asian countries we visited are more dependent on public transportation than most U.S. residents and therefore, according to the rail operators we spoke with, may be more willing to accept more intrusive security measures, simply because they have no other choice for getting from place to place. Nevertheless, in order to identify innovative security measures that could help further mitigate terrorism-related risk to rail assets—especially as part of a broader risk management approach discussed earlier—it is important to at least consider assessing the feasibility and costs and benefits of implementing the three rail security practices we identified in foreign countries in the United States. Officials from DHS, DOT, passenger rail industry associations, and rail systems we interviewed told us that operators would benefit from such an evaluation. Furthermore, the passenger rail association officials told us that such an evaluation should include practices used by foreign rail operators that integrate security into infrastructure design.

Differences in the business models and financial status of some foreign rail operators could also affect the feasibility of adopting certain security practices in the United States. Several foreign countries we visited have privatized their passenger rail operations. Although most of the foreign rail operators we visited—even the privatized systems—rely on their governments for some type of financial assistance, two foreign rail operators generated significant revenue and profits in other business endeavors, which they said allowed them to invest heavily in security measures for their rail systems. In particular, the Paris Metro system is operated by the RATP Corporation (Régie Autonome des Transports Parisiens), which also contracts with other cities in France and throughout the world to provide consulting and project management services. RATP's ability to make a profit, according to its officials, through its consulting services allows the agency to supplement government funding in order to support expensive security measures for the Paris mass transit system. For example, RATP recently installed a computer-assisted security control system that uses CCTV, radio, and global positioning technology that it says has significantly reduced the amount of time it takes for security or emergency personnel to respond to an incident or emergency, such as a terrorist attack. Because of RATP's available funding for security, the corporation also purchased an identical system for the Metropolitan Paris Police, so the RATP and the police system would be compatible. In contrast, domestic rail operators do not generate a profit and therefore are dependent on financial assistance from the Federal, State, and local levels of government to maintain and enhance services, including funding security improvements.

Another important difference between domestic and foreign rail operators is the structure of their police forces. In particular, England, France, Belgium, and Spain all have national police forces patrolling rail systems in these countries. The use of a national police force is a reflection that these foreign countries often have one nationalized rail system, rather than over 30 rail transit systems owned and operated by numerous state and local governments, as is the case in the United States. For example, in France, the French National Railway operates all intercity passenger rail services in the country and utilizes the French Railway police to provide security. According to foreign rail operators, the use of one national rail police force allows for consistent policing and security measures throughout the country. In the United States, in contrast, there is not a national police force for the rail transit systems.[32] Rather, some transit agencies maintain individual police forces, while others rely on their city or county police forces for security.

Conclusions

In conclusion, Mr. Chairman, we are encouraged by the steps DHS components have taken to use elements of a risk management approach to guide critical infrastructure protection decisions for the passenger rail industry. However, enhanced Federal leadership is needed to help ensure that actions and investments designed to enhance security are properly focused and prioritized, so that finite resources may be allocated appropriately to help protect all modes of transportation and secure other national critical infrastructure sectors. Leadership on this issue should reflect the shared responsibilities required to coordinate actions on the part of Federal, State, and local governments; the private sector; and rail passengers who ride these systems.

Specifically, both DHS and TSA could take additional steps to help ensure that the risk management efforts under way clearly and effectively identify priority areas for security-related investments in rail and other sectors. We recognize that TSA has had many aviation security-related responsibilities and has implemented many security initiatives to meet legislative requirements. Notwithstanding, TSA has not yet completed its methodology for determining how the results of threat, criticality, and vulnerability assessments will be used to identify and prioritize risks to passenger rail and other transportation sectors. In order to complete and apply its methodology as part of the forthcoming transportation sector-specific plan, TSA needs to more consistently involve industry stakeholders in the overall risk assessment process and collaborate with them on collecting and analyzing information on critical infrastructure and key resources in the passenger rail industry. Without consistent and substantive stakeholder input, TSA may not be able to fully capture critical information on rail assets—information that is needed to properly assess risk. In addition, as part of the process to complete its risk assessment methodology, TSA needs to consider whether other proven approaches, such as ODP's risk assessment methodology, could be leveraged for rail and other transportation modes, such as aviation. Until the overall risk to the entire transportation sector is identified, TSA will not be able to fully benefit from the outcome of risk management analysis—including determining where and how to target the Nation's limited resources to achieve the greatest security gains.

Once risk assessments for the passenger rail industry have been completed, it will be critical to be able to compare assessment results across all transportation modes as well as other critical sectors and make informed, risk-based investment trade-offs. The framework that DHS is developing to help ensure that risks to all sectors can be analyzed and compared in a consistent way needs to be completed and shared with TSA and other sector-specific agencies. The delay in completing the element of the framework that defines concepts, terminology, and metrics for assessing risk limits DHS's ability to compare risk across sectors as sector-specific agencies are concurrently conducting risk assessment activities without this guidance. Until this framework is complete, it will not be possible for information from different sectors to be reconciled to allow for a meaningful comparison of risk—a goal outlined in DHS's interim NIPP.

Apart from its efforts to formally identify risks, TSA has taken steps to enhance the security of the overall passenger rail system. The issuance of security directives in the wake of the Madrid bombings was a well-intentioned effort to take swift action in response to a current threat. However, because these directives were issued under emergency circumstances, with limited input and review by rail industry and Federal stakeholders—and no public comment period—they may not provide the industry with baseline security standards based on industry best practices. Nor is it clear how these directives are to be measured and enforced. Consequently, neither the Federal Government nor rail operators can be sure they are requiring and implementing security practices proven to help prevent or mitigate disasters. Collaborating with rail industry stakeholders to develop security standards is an important starting point for strengthening the security of passenger rail systems.

While foreign passenger rail operators face similar challenges to securing their systems and have generally implemented similar security practices as U.S. rail operators, there are some practices that are utilized abroad that U.S. rail operators or the Federal Government have not studied in terms of the feasibility, costs, and benefits. For example, an information clearinghouse for new passenger rail technologies that are available and have been tested might allow rail operators to efficiently implement technologies that had already received approval. In addition, while FTA plans to require rail operators to consider its security infrastructure design guidelines when renovating or constructing rail systems or facilities, opportunities may still exist to further research and evaluate ways of integrating security into design, as some foreign rail operators have done. Another rail security practice—covert testing of rail security procedures—is being used in two foreign rail systems we visited and is considered by them as an effective means of keeping rail employees alert to their surroundings and potential security threats. And finally, random searches of passengers and baggage are being used by two foreign rail operators and this practice has recently been adopted by four domestic rail operators in the wake of the London attacks.

Introducing these security practices into the United States may involve cultural, financial, and political challenges, owing to differences between the United States and foreign nations. Nonetheless, as part of the overall risk management approach, there may be compelling reasons for exploring the feasibility, costs, and benefits of implementing any of these practices in the United States. Doing so could enable the United States to leverage the experiences and knowledge of foreign passenger rail operators and help identify additional innovative measures to secure rail systems against terrorist attack in this country.

In our recently issued report on passenger rail security, we recommended, among other things, that to help ensure that the Federal Government has the information it needs to prioritize passenger rail assets based on risk, and in order to evaluate, select, and implement commensurate measures to help the Nation's passenger rail operators protect their systems against acts of terrorism, TSA should establish a plan with timelines for completing its methodology for conducting risk assessments and develop security standards that reflect industry best practices and can be measured and enforced, by using the Federal rule-making process. In addition, we recommended that the Secretary of DHS, in collaboration with DOT and the passenger rail industry, determine the feasibility, in a risk management context, of implementing certain security practices used by foreign rail operators. DHS, DOT, and Amtrak generally agreed with the report's recommendations.

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

ENDNOTES

[1] Pub. L. No. 108–458, 118 Stat. 3638.

[2] GAO, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO–05–851 (Washington, D.C.: Sept. 9, 2005).

[3] The American Public Transportation Association compiled this Fiscal Year 2003 ridership data from FTA's National Transit Database. These are the most current data available. Rail transit systems in the District of Columbia and Puerto Rico are included in these statistics.

[4] The Alaska Railroad Corporation also operates intercity passenger rail service.

[5] Pub. L. No. 107–71, 115 Stat. 597 (2001).

[6] Pub. L. No. 107–296, 116 Stat. 2135 (2002).

[7] The Department of Justice established ODP in 1998 within the Office of Justice Programs. ODP was subsequently transferred to DHS's Directorate of Border and Transportation Security upon DHS's creation in March 2003 (Homeland Security Act of 2002, section 403(5), 6 U.S.C. 203(5)). In March 2004, the Secretary of Homeland Security consolidated ODP with the Office of State and Local Government Coordination to form the Office of State and Local Government Coordination and Preparedness (SLGCP). SLGCP, which reports directly to the DHS Secretary, was created to provide a "one-stop shop" for the numerous Federal preparedness initiatives applicable to state and local governments.

[8] At the time of our review, DHS was undertaking a department-wide reorganization that will affect both the structure and the functions of DHS directorates and component agencies.

[9] Pub. L. No. 108–334, 118 Stat. 1298 (2004).

[10] FRA administers and enforces the Federal laws and related regulations that are designed to promote safety on railroads, such as track maintenance, inspection standards, equipment standards, and operating practices. FRA exercises jurisdiction over all areas of railroad safety under 49 U.S.C. 20103.

[11] Pub. L. No. 108–458, 118 Stat. 3638.

[12] GAO, *Transportation Security: Systematic Planning Needed to Optimize Resources*, GAO–05–357T (Washington, D.C.: Feb. 15, 2005); *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO–02–208T (Washington, D.C.: Oct. 31, 2001); and *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments*, GAO/NSIAD–98–74 (Washington, D.C.: April 9, 1998).

[13] Sector-specific agencies have been designated for the following sectors: transportation; agriculture and food; public health and health care; drinking water and wastewater treatment; energy; banking and finance; national monuments and icons; defense industrial base; information technology; telecommunications; chemical; emergency services; postal and package shipping; dams; government facilities; commercial facilities; and nuclear reactors, materials, and waste.

[14] The transportation sector includes mass transit; aviation; maritime; ground/surface; and rail and pipeline systems.

[15] ODP has completed risk assessments with the Port Authority of New York and New Jersey, New Jersey Transit, Massachusetts Bay Transportation Authority, Washington Metropolitan Area Transit Authority, Southeastern Pennsylvania Transportation Authority, Tri-County Metropolitan Transportation District of Oregon, and the Delaware River Port Authority.

[16] PANYNJ is a bi-state public agency that manages and maintains bridges, tunnels, bus terminals, airports, the PATH passenger rail system, and seaports in the greater New York/New Jersey metropolitan area. PANYNJ was also the property owner and operator of the World Trade Center site and the PATH passenger rail station underneath the site that was destroyed by the September 11 terrorist attacks. At the request of PANYNJ, ODP's technical assistance team worked with authority personnel to conduct the first risk assessment using ODP's model. This collaborative effort provided the means for ODP to test and refine its methodology and develop the tool kit now in use.

[17] The Association of American Railroads is an association representing the interests of the rail industry, focused mostly at the Federal level. Its members are primarily freight rail operators in the United States, Canada, and Mexico. However, it also represents some passenger rail interests, including Amtrak.

[18] The American Public Transportation Association is a nonprofit trade association representing over 1,500 public and private member organizations, including transit systems and commuter rail operators; planning, design, construction, and finance firms; product and service providers; academic institutions; transit associations; and state departments of transportation.

[19] Up to 30 percent of the available funds will be available to assist Amtrak in meeting its most pressing security needs in the Northeast Corridor and Chicago (as

identified through previously conducted site-specific assessments) prior to completion of the risk assessment. However, the remainder of the grant funds will not be released until Amtrak has completed the risk assessment and also submitted a security and emergency preparedness plan. Amtrak is also required to demonstrate that its planning process and allocations of funds are fully coordinated with regional planning efforts in the National Capitol Region, Philadelphia, New York, Boston, and Chicago. Amtrak is using approximately $700,000 of the grant funds for the ODP risk assessment.

[20] The results of TSA's passenger and freight rail threat assessments contain information that is security sensitive or classified and therefore cannot be disclosed in this testimony.

[21] DHS refers to this framework as a Risk Analysis and Management for Critical Asset Protection.

[22] According to TSA, in issuing the passenger rail and mass transit security directives, TSA exercised its authorities under 49 U.S.C. 114. We are currently examining whether TSA met all relevant legal requirements in the promulgation of the directives.

[23] 49 CFR 238.235.

[24] These positions were funded through the DHS Appropriations Act of 2005 and its accompanying conference report, which provided TSA with $12 million in funding for rail security activities.

[25] Congress required that an annex to the MOU be signed that would, among other things, define and clarify the respective transit security roles and responsibilities of each department. Pub. L. 109–59, § 3028 (2005).

[26] APTA is a standards development organization recognized by DOT that has set standards for commuter rail, mass transit, and bus safety and operations.

[27] At the time we completed our work in June 2005, these three practices were not utilized. However, as discussed later in this report, some rail operators began using random screening in the aftermath of the July bomb attacks on the London subway system.

[28] As we have previously reported, since the mid-1990s, Federal funding for transit and commuter rail operators has generally been limited to assistance with capital projects involving building new transit service, extensions of existing lines, or rehabilitation of existing transit infrastructure, such as tracks, rolling stock, or stations. See GAO–03–263.

[29] Actions taken by Amtrak to enhance security are discussed later in this testimony.

[30] GAO–03–843.

[31] See GAO–03–843.

[32] Unlike domestic rail transit agencies, Amtrak maintains a 342-member police force for its national network.

The CHAIRMAN. Thank you very much. Senator McCain, do you have an opening statement or questions?

Senator MCCAIN. I follow you, Mr. Chairman. After you, sir.

The CHAIRMAN. All right, let me just put it this way to all of you. We sought to assure that we would have jurisdiction over TSA, rail security and other aspects in this Committee because of the existence of the authorities that Mr. Boardman has just mentioned concerning FRA and existing systems prior to the reorganizations that brought about TSA. But it appears that we are still going along two roads. You talk about coordination, but what about consolidation? It seems to me that this is going to be extremely confusing to everybody in the railroad industry if we don't find one way to deal with this. Now, the solution of the 9/11 Commission was to just wipe out FRA as far as security is concerned and our solution was to try and bring it together so that we'd have a comprehensive system for improving rail security but not have duplicated functions that require coordination.

Now, how are we going to get it together? And Mr. Hawley, notwithstanding what Ms. Berrick said—I thought that was kind of complimentary that you are trying to work on risk assessment but you haven't accomplished anything yet. When can we expect that risk assessment and when can we expect a plan to put together the system so that there's one coherent system for safety on our railroads?

Mr. HAWLEY. Yes, sir. On the risk management approach, we use that today. I think what we are referring to there, are specific major models that are very complex that are useful but are not really the operational drivers in terms of a flexible risk and a flexible network. So we use absolutely the risk-based approach on a daily basis on operational matters as well as we devote our investment resources.

The CHAIRMAN. If you are doing that every day what's Mr. Boardman doing? He says they're in charge.

Mr. HAWLEY. Well, Mr. Boardman is in charge of safety and we have a very good working relationship that I think, that the report that Ms. Berrick referred to is highly instructive, highly useful, and as I was preparing for my confirmation before this Committee, I had the opportunity to review it and the comments there about single point of contact, being connected, one voice from the Federal Government to the industry or the transit community is one that we whole-heartedly adopt. And, in fact, Secretary Chertoff recently approved a reorganization of the entire agency to enable us to speak with one voice to these communities.

The CHAIRMAN. What agency? Your agency?

Mr. HAWLEY. Yes, sir, TSA. And to plug into FRA on a daily basis and build institutional connections among us so it doesn't depend on a good relationship among administrators, but the actual work process of the two agencies take advantage, certainly from our point of view, of the expertise that the FRA has and expect that the good working relationship that we've had to this point will continue to evolve to be even better coordinated and reflected in the work process.

The CHAIRMAN. Mr. Boardman, what do you say?

Mr. BOARDMAN. I think that, Mr. Chairman, I do think FRA and TSA, especially since Mr. Hawley has come onboard, have been able to work in a very hand-in-glove fashion, especially with their inspectors out in the field today. I think there is a difference between safety and security in a couple of ways. Safety in terms of thinking about it, it's really being certain that adverse effects will not be caused by some agent under defined conditions. In other words, when the FRA puts its standards and its activity together there are some risks, and terrorism against the passenger train is beyond the conditions that FRA really considered when it set those standards in the past. One of the difficulties, I think, with security has been that it's not only being free from danger and injury, it's also being free from anxiety and fear. And, I think that there is a need for us to work together as a Federal Government to find a way to find those conditions, those adverse effects that we can't establish in terms of a process or effective conditions that, as I think Mr. Hawley talked about, that keep terrorists off balance in terms of how we look at this thing for the future. I think that we have an important role in the FRA in security because we benefit security because we don't differentiate what that agent is that causes a catastrophic event. It could be a broken rail from a joint fracture, it could be vandals, it could be something more sinister, but there are those risks that are beyond that and we want to work with DHS to resolve that.

The CHAIRMAN. John?

STATEMENT OF HON. JOHN McCAIN, U.S. SENATOR FROM ARIZONA

Senator MCCAIN. Thank you, Mr. Chairman. Along the lines of what the Chairman was just asking, tell me Mr. Hawley and Mr. Boardman, who is in charge?

Mr. HAWLEY. For security, TSA is in charge and for safety it's FRA. It is very similar with FAA and TSA. So, it's a similar pattern that we have throughout the transportation sector.

Senator MCCAIN. Ms. Berrick, does that seem workable to you?

Ms. BERRICK. I think it is today. About a year ago we did some work and talked to rail operators. They felt that the role between FRA and TSA wasn't always very clear to them. One of the recommendations we made coming out of that work was that the Department of Transportation and the Department of Homeland Security establish a Memorandum of Understanding, clearly delineating roles and responsibilities and they did that about a year ago. And recently, last month they signed a Transit Security Annex to that MOU which I think further delineates roles and responsibilities.

So I think they've gone a long way and are being more clear on who's responsible for rail security.

Senator MCCAIN. Well, apparently, it's not clear to the Association of American Railroads because they submit testimony that they will present that says TSA and FRA should clarify which agency has ultimate responsibility for which aspects of rail safety and security. Today, the allocation of responsibilities is not always clear, so the people that they are serving are not that clear, at least according to Mr. Hamberger's testimony.

Ms. Berrick, are we devoting sufficient funds to rail security today? My information is, this year's Homeland Security Appropriations bill appropriated $150 million for intercity passenger rail transportation, freight rail and transit security grants. Senator Lieberman, recently noted that while the government has spent about $15 billion in aviation securities since September 11th, about $300 million has been spent on mass transit security. Does this seem a little unequal particularly in light of the Madrid attacks and other threats to rail security both in America and overseas?

Ms. BERRICK. I think if you look at TSA's budget which is about $3.9 billion and within TSA, in addition to the $150 million at the DHS level, within TSA there is $8 million that's devoted to higher additional rail inspectors this year. So I think, if you just look at the budget, that certainly raises questions about whether or not that's an appropriate amount. I don't think that anybody can really answer the question right now, What is the appropriate amount to devote to rail security? Just because the risk assessment——

Senator MCCAIN. I'm not asking for an appropriate amount, I'm asking if whether we are spending enough?

Ms. BERRICK. Yes, I would say that you can't answer that question right now. I don't know the answer because DHS hasn't completed these risk assessment efforts to identify where the vulnerabilities are that need to be fixed. And I think, until they do that in any systematic way, it really can't be estimated what they need.

Senator McCAIN. Well, in all due respect, Mr. Hawley, the year is 2005 and we still haven't made an assessment yet?

Mr. HAWLEY. No, sir, we have and it gets to the question of protecting infrastructure which is different. Which is a solid definable place geographically with defining a flexible transportation network where in the New York City Transit System alone, I'm sure if you know this, four and a half million passengers a day going in and out of 400 and some——

Senator McCAIN. And it still remains a question of the security of the tunnels as well.

Mr. HAWLEY. Well, it's almost certainly a piece of that but we have taken the whole network of transportation and all the modes because it is an open system. It is vulnerable and as you know, the targeting can be flexible and adaptive. So, if we were publishing a list of the top 100 things in priority that we're allocating our resources to, that is too simple a guide to give to somebody else and I think we go back to the person connecting the dots on CBP, and ICE, and FBI to find the person, before the attack is in progress against a particular transit system or aviation target.

Senator McCAIN. What are your priorities without comprising security?

Mr. HAWLEY. Sure, it is absolutely to do what is possible to identify the terrorist in advance which can be done and how you do that specifically is with connecting the information systems that we have within DHS, the Customs and Border Protection as well as us and ICE and FBI and the reporting we get from industries, suspicious incidents.

Senator McCAIN. I need to rephrase my question, without compromising security, what are your highest priorities for defending?

Mr. HAWLEY. For the, essentially aviation would be the highest priority.

Senator McCAIN. As far as rail security is concerned.

Mr. HAWLEY. For rail security it gets to first, establishing that unlike aviation which is operated by the Federal Government, rail is operated by either transit systems or railroads and to first establish what they are doing. Then, if what they are doing makes sense and then are they doing what they say they are doing? All of those things have——

Senator McCAIN. I'm still asking what your priorities are. Is it the tunnels, is it New York City, is it New Mexico? I'm asking which areas need to be addressed first. You have to prioritize. I remember right after 2001, one of the highest priorities that was given to this Committee were the tunnels that connect on the eastern corridors.

Mr. HAWLEY. Yes.

Senator McCAIN. So.

Mr. HAWLEY. We are very focused on tunnels in New York and elsewhere and look at things that would be effective against tunnels wherever they are but clearly, the New York City area is very visible as is the D.C. Metro area in the northeast corridor there. There are priorities within that but the——

Senator MCCAIN. I'm sorry to interrupt, Mr. Hawley. But, it's hard for us to recommend authorization and appropriations in a prioritized fashion since clearly, we can't fund everything until we get your priorities.

Mr. HAWLEY. Yes.

Senator MCCAIN. Do you see my point?

Mr. HAWLEY. Yes, yes, sir, and the way the President's budget is put together, puts a lot of, now the decisionmaking at the state and local level where they can make the operation tradeoffs as to——

Senator MCCAIN. And that assumes then that they don't want any Federal money. I'm saying is, if it's Federal dollars we have to know what the Federal priority is.

Mr. HAWLEY. Yes.

Senator MCCAIN. If they, if local authorities want to set their priorities and fund them, that's fine with us. OK? I'm still having trouble getting your priorities which would then help us, as we go through the authorizing and appropriating process.

Mr. HAWLEY. Sure, OK, information, communication, training, drilling, preparedness——

Senator MCCAIN. I'm talking about areas that need specific priorities. I understand that education and training and communication are very important. That's why we are about to have a big fight over allocation of spectrum.

Mr. HAWLEY. Yes, sir, so you want the geography or the part of the train system or——

Senator MCCAIN. Is it New York tunnels? Is it the West Coast rail network? Is it the Union Station here? I just think we need to know some priorities if we are going to earmark specific funds for specific purposes.

Mr. HAWLEY. Yes, sir.

Senator MCCAIN. We're just going to give you a whole bunch of money and say spend it however you want, then it doesn't matter. But I don't think we are going to do that.

Mr. HAWLEY. No, sir. But the flexibility and adaptability of the resources we have is critical. So, for instance, we have resources like canine teams, that we have on a mobile basis so that in a situation where——

Senator MCCAIN. Is that your highest priority?

Mr. HAWLEY. It's not my highest priority.

Senator MCCAIN. Well, that's what I keep asking, Mr. Hawley.

Mr. HAWLEY. OK, it is, it's the flexible resources to be able to——

Senator MCCAIN. All right, Mr. Hawley then I will submit on the floor an amendment for flexible resources. I'm sorry that you aren't more forthcoming. Mr. Chairman, I know there are other witnesses. You are very unforthcoming, Mr. Hawley and I am very disappointed.

The CHAIRMAN. Well, let me follow on to what Senator McCain has discussed, we also oversee airline transportation and airline transportation has been funded as far as security concepts are concerned primarily by increased taxes on passengers. I have not seen any recommendation from anyone that the people who use rail transportation should pay a portion of the cost of providing their own security. Have you examined this? Any one of you examine why it is that we can't ask the rail passenger to pay as the airline passenger pays for at least part of the security we are trying to provide?

Mr. HAWLEY. Yes, it's done. That's where the money comes out of the local level and part of the fare box goes to programs from the local level that affect security.

The CHAIRMAN. Have you recommended any increase in cost to the passengers for rail security?

Mr. HAWLEY. No, sir.

The CHAIRMAN. Have you, Mr. Boardman?

Mr. BOARDMAN. No, Mr. Chairman. I wouldn't recommend that.

The CHAIRMAN. Why?

Mr. BOARDMAN. Most transit systems in operation today don't cover their operating costs. Most of them in rural areas cover as much as maybe 30 or 40 percent of their costs. When you're in New York City itself, you might be as high as 70 percent of its costs. So today——

The CHAIRMAN. That's looking at it the wrong way. Do you know what gasoline costs today post-9/11?

Mr. BOARDMAN. Yes, sir.

The CHAIRMAN. The people who are driving cars, the people who are flying are all paying increased costs. Why is it that railroad passengers are such preferred characters that they can't pay a portion of these costs? Everyone seems to be turning to the Federal Government for the total support of the security system for rail.

Mr. BOARDMAN. I understand sir.

The CHAIRMAN. Why?

Mr. BOARDMAN. I think that all transit systems today receive Federal assistance and they do that because they lose money.

The CHAIRMAN. Well, almost every airline in the country is in bankruptcy now and has been since 9/11 because of the increased costs put on airlines themselves in addition to the increased cost to the passengers. But, we haven't seen any increased burden put on the passengers for rail transportation. Ms. Berrick, have you looked at that?

Ms. BERRICK. Well, we did look at who pays for rail security and found that it is really shared between the Federal Government, State and locals who own a lot of the transit and then also the private sector. The American public——

The CHAIRMAN. Wait, back up. The allocation to them is still based upon pre-9/11 fares, isn't it? Have you seen any increase in the cost of rail transportation?

Ms. BERRICK. We didn't look at the actual fares and the increases over time.

The CHAIRMAN. Why not?

Ms. BERRICK. The objective of our study was to see what was being done first of all within the U.S. to secure passenger rail and whether or not there were any practices in foreign countries that we could apply here to secure the rail system. We also looked in a general sense of what's been spent on rail security on the Federal level, not a whole lot of money last year, about $150 million in grants. The American Public Transportation Association estimated that since 9/11 the private sector, the private rail operators, spent about $1.7 billion on security. So I think the rail operators themselves through fees are devoting a lot to security.

The CHAIRMAN. It seems like just a simple matter of economics to me that with the increase in price of gasoline people who would otherwise drive from here to New York are going to go by train. Right? There's not been any increase in cost to go by train. So you have to plan for increased burdens on the rail transportation system because the increased cost of alternative means of transportation, both air and auto or bus has increased substantially. Rail has not. And yet we are hearing we have to have more money to protect those people who are riding the rails.

Ms. BERRICK. I think what the highest priority should be, in my opinion, for the Department is to complete their risk assessment efforts. It's right, TSA has started these efforts. They haven't yet completed them. The Department level, they also have risk assessments. They need to be coordinated to determine, first of all, what's the requirement——

The CHAIRMAN. I would accept your concept of risk assessment. I think we all do. That should be the number one priority. But, the question of who's going to pay for the changes that are necessary ought to be primary too, shouldn't it?

Ms. BERRICK. I think it should and I think the first step is the risk assessment to determine how much do we actually need and where we need to focus our money.

The CHAIRMAN. Well, meanwhile you are just attracting more and more people to the rail transportation system, aren't you? If airline costs are going up and transportation by bus or by automobile is going up, isn't it natural that people are going to go where prices are not going up?

Ms. BERRICK. That's possible and we did not study the pricing.

The CHAIRMAN. Would you study that just to see if I'm right?

Ms. BERRICK. OK, we'll look at that and get back with you. Thank you.

Senator MCCAIN. Mr. Chairman, could I just make one addition?

The CHAIRMAN. Yes, sir.

Senator MCCAIN. Mr. Hawley, I understand you have a very tough job and I don't mean to be too hard on you but we really need to have a sense of your priorities. If that has to be done in a classified fashion so that the Members of this Committee can know what you want, I'd be glad to understand that aspect of national security, but I think it would help us, because we are going to engage in some prioritization ourselves, and I think it is important for us that you provide that information.

Mr. HAWLEY. Yes sir.

Senator MCCAIN. I thank you, Mr. Chairman.

The CHAIRMAN. I join in that request. I'd also like to know if you can tell us, I admire the way New York City handled the crisis after the London catastrophe in rails but they really started a system of really improving inspection, for anyone who went onboard those subways or their trains. But, I also understand that there is an increased allocation to pay for that service and I wonder why? I come from a state where 90 percent of travel is by plane and our people are paying—although we are a very small state, our people are paying a substantial increase in costs every month it seems.

The people that are using these massive transportation systems down here, they are not paying any increased costs for security at all and I think that's not only unfair but it's not wise. That means that unless, as Senator McCain says, we outline some more money to allocate to these systems, they are not going to get the securities required to maintain the securities necessary for that mode of transportation. Senator Boxer?

STATEMENT OF HON. BARBARA BOXER, U.S. SENATOR FROM CALIFORNIA

Senator BOXER. Thank you. I am so sorry that I was late, I was at a meeting about Hurricane Katrina aftermath relief, I am really sorry. Mr. Chairman, thank you very much for holding this hearing.

A new GAO report, which Senator Snowe and I requested, shows that the Transportation Security Administration has not adequately secured America's passenger railways and it's not for lack of warning. We've seen what's happened in Madrid, we saw what happened in London, we know because we've had access to documents that show that the trains are definitely on the al-Qaeda lists. So, it seems to me, Mr. Chairman, we've ignored warning after warning and I say "we", I don't really mean this Committee, Mr. Chairman. I'd like to show you a chart that I made up here if I could.

Mr. Chairman, I just wanted to share with you a chart because I think that this Committee under Senator McCain's leadership before has acted on this issue a couple of times and I just wanted to note it. In 2001, the Commerce Committee approved the Rail Security Act of 2001. No action was taken by the full Senate, and then in 2004 the Commerce Committee approved the Rail Security Act of 2004. The full Senate approved that Rail Security Act but then the House didn't act. So, I think this Committee has tried very hard to do something but we haven't had the entire Congress going.

So, I think what we need to do is get on with it. I want to talk about my state which has the second-highest Amtrak ridership in the country and I see Senator Lautenberg here, but people don't recognize that California has a very large Amtrak ridership. Almost nine million passenger trips began or ended in California during 2004. Amtrak operates an average of 70 intercity and 200 commuter trains per day in California. So, when people think Amtrak, they think East Coast, they've got to say West Coast because we are the second largest ridership.

In addition, the freight rail system is extremely important for goods movement throughout the country. California ports receive over 40 percent of all the goods that are shipped into the U.S.; the ports of L.A. and Long Beach comprise the largest port complex in the U.S. and they are crucial for our Nation's economy.

Now, here's what happens, Mr. Chairman. The goods arrive and then they are taken by train throughout the country, and once these trains emerge through the Alameda Corridor, which is in the Los Angeles area, they often cross a road where there is no grade separation. So, grade separation is another critical issue because if there were to be a terrorist attack and those grades are blocked, we cannot get the emergency vehicles through.

So, Mr. Chairman, I once again thank you for having this hearing. I understand it was pretty contentious before I got here but I just want to say we expect more from this Administration; we have to. It's not that we are being argumentative. It's that we've been warned. How many times do we have to be warned? We've seen al-Qaeda documents, we saw what happened in Madrid, we saw what happened in London, we saw what happened recently and rumors spread in New York and there's lots more we can do. We can't 100 percent protect anything, any asset. But we can surely do better. GAO makes that point and I'm just hopeful that you will read that report and you will move to finally secure our Nation's rail system because we've been warned and how many times could we get away with this? Not too many more times. Thank you.

Senator LAUTENBERG. Mr. Chairman, may I?

The CHAIRMAN. Senator Boxer, are you finished?

Senator BOXER. I'm finished with my statement.

The CHAIRMAN. Thanks. Senator Lautenberg?

STATEMENT OF HON. FRANK R. LAUTENBERG, U.S. SENATOR FROM NEW JERSEY

Senator LAUTENBERG. Yes, thanks, Mr. Chairman, and thanks to you and Senator McCain, we're moving legislation, trying arduously to move legislation. We look back and I don't want to be repetitive if things have been said before that have taken care of some of the issues. But when we look forward at the vulnerability that we have as a result of possible hazardous cargo being transported or materials being carried and not really facing up to the reality of what we've got to do to protect ourselves. Particularly obvious is the railroad track that sits right here at the Capitol. We in New Jersey are so dependent on transit and passenger rail service and I'm just wondering why it is that when we've seen these incidents pass before in London, Madrid? Why is it that we are still waiting here for a plan by our government to do something about it, to make the investment that is necessary?

What we saw in Graniteville, South Carolina, hazmat releases can have the same effect as a weapon of mass destruction. Now what's TSA doing to track the thousands of hazmat rail cars each day? Secretary Hawley, does the Administration believe that active monitoring of the movement of these cars in necessary?

Mr. HAWLEY. Yes sir, and that is done in the current setup by the companies themselves and in the circumstance where we would require access to the specific location of individual trains or cars or shipments, that is something we can get from them.

Senator LAUTENBERG. How do we monitor the quality of their security? Years ago the screening at aviation destinations was done by airlines and we found that they were quite inadequate. So, the government stepped in and said, "OK, private sectors had its end, they haven't done a good job. We are going to come in here and we're going to do it." What's the difference, Mr. Hawley, between that situation and the current need?

Mr. HAWLEY. In regards to freight rail? As regard to freight rail, the consequences of a safety problem or a terrorist act against—involving hazardous material can be the financial death penalty for a freight railroad and so they are highly motivated for a lot of reasons to do what is necessary to prevent that happening and what we do to monitor that, we do the trust/verify approach to have security reviews to understand what it is they do and then verify in fact, that they are doing it.

Senator LAUTENBERG. Well, if we looked at Texarkana, the train derailment there is an example, it's quite recent, about a week ago. Hundreds of homes were evacuated after seven empty train cars and a tanker containing propylene, derailed in a switch yard, exploding in a ball of fire. Initially, the police thought that the chemical involved was vinyl acetate which releases poisonous fumes and officers went door to door urging thousands of people in a two by five mile area to move to the north side of town and I think it once again, does say we've got to make certain if we are going to rely entirely on the private sector that things are done in a fashion that protects the people in the areas.

So, I think that is something that has to be looked at and I would appreciate getting some data about what it is precisely that the government does to check to see if these things are done.

Mr. Chairman, I'm anxious to hear the next panel and I'm finished with mine.

The CHAIRMAN. Thank you. Senator Boxer, you have an additional question?

Senator BOXER. I just have one question to ask to Mr. Hawley and Mr. Boardman, whoever feels comfortable doing it. One of the ways that I am told back home we can really help the situation is to have enough canine patrols because they're pretty effective. What do you think the needs are in terms of dollars to provide for canine patrols?

Mr. HAWLEY. Yes, ma'am, I believe that the canine patrol is an excellent flexible and adaptive security measure that can be used in a transit environment, aviation environment, and we recently did a test with the inter-city bus environment. So, that is an important aspect of our program. We've recently increased from the 340 range up to—we're now going to be close to about 450 dog teams and we, in addition——

Senator BOXER. How many dogs in a team?

Mr. HAWLEY. Three.

Senator BOXER. And we have 450 operational now, teams?

Mr. HAWLEY. Yes, 420 now. We have added through a program that people are in training now, 30 additional dogs or 10 teams for specifically transit including four in California.

Senator BOXER. Are these all for Amtrak?

Mr. HAWLEY. These are for transit agencies and for Amtrak, we are working with Amtrak to make it operationally smooth for us to deploy dog teams from either other locations or from airports, other cities.

Senator BOXER. Do you know what Amtrak says it needs for dog teams?

Mr. HAWLEY. I don't know the dollar number, no.

Senator BOXER. OK, well they need $156 million additional to secure their largest stations, so I would appreciate if you would talk with them so that you know what it is that they need because they are telling us. They should be telling you or you should be asking them.

Mr. HAWLEY. We do have conversations about it at all levels.

Senator BOXER. OK. Well, Mr. Chairman, I just think—I just say that Amtrak is saying and they will tell us, they need $156 million in additional funds to secure the largest stations with canine teams and I'm just saying $156 million, given the tragedies that could befall us, it's a small investment. Every time a car comes in here, Senators or otherwise, they bring out a canine team and it seems that the officers feel very confident and comfortable with that and it seems with all the high tech equipment we have, as you say Mr. Hawley, using canine teams works for a relatively small amount of money. So, I'm done with my questions but I hope that you'll get with the Amtrak people.

Senator LAUTENBERG. Mr. Chairman, my colleague elicits a question for me, if you don't mind, about the same subject. Mr. Hawley, the Secretary of Transportation or his designee sits on the Amtrak Board. In April, the Board approved Amtrak's funding request for its security and needs up to $254 million a year. If this funding was needed to help secure Amtrak and the 25 million people who ride it annually, why didn't the President ask for that in the budget?

Mr. HAWLEY. TSA, I'll speak for TSA, has the multi-modal responsibility and as such, we view—I view and our team views that Amtrak is very much within the zone that we worry about and without regard to whether we have specific Amtrak programs that we use programs we have for other modes including Federal Air Marshals to be available for opportunities that may be required for Amtrak. As well, as we mentioned the canine teams and even more broadly than that is the whole area of information sharing and intelligence sharing that I think, as far as TSA is concerned, Amtrak is very, very high on the priority list on an operational level and we work on that on a very intensive basis.

The CHAIRMAN. Thank you, Senator, we are going to have to move on.

Mr. HAWLEY. Yes, OK.

The CHAIRMAN. I wish you the best, I would ask that you provide us with a list of the cost of passengers on the major rail systems which you are talking about, what Amtrak and other passenger systems throughout the country on a basis of—let's go back about 4 years and bring it forward. To what extent have any of those people been asked to pay any portion of increased cost to safety and security. Thank you all very much but we will have to turn to the next witness list.

Ms. BERRICK. Thank you.

Mr. HAWLEY. Thank you.

STATEMENT OF EDWARD R. HAMBERGER, PRESIDENT/CEO, ASSOCIATION OF AMERICAN RAILROADS

Mr. HAMBERGER. I appreciate the opportunity to be here to discuss freight railroad security with the Committee. The safety and security of hazardous materials transportation, of course, is of the utmost concern to the Nation's industry and perhaps to this Committee as well so, let me move right into that issue.

As common carriers, let me emphasize that railroads are required by Federal law to move hazardous material and we move it in the safest, most efficient way possible. In fact, we have a very good safety record notwithstanding the fact that accidents do occur. In 2003, we moved 1.7 million carloads of hazardous materials—99.998 percent of those shipments arrived at destination without any release from an accident along the way.

Railroads are sensitive to the concerns of those who live along rail lines and we take very seriously our obligation to move hazardous materials safely and securely. We assist communities in developing and evaluating emergency response plans and help train more than 20,000 emergency responders each year. We provide local emergency responders with a list of the most dangerous chemicals likely to be moved through their communities and work with the chemical manufacturers, shippers and tank car suppliers to improve operating procedures and tank car safety.

As you are aware, Washington D.C. has enacted legislation to ban hazmat shipments over certain routes. Other cities, Baltimore and others, are considering such bans. Legislation has been proposed in Congress to force rerouting of hazardous materials. We believe that is the wrong approach to take. Local transit bans would not eliminate the risk inherent in moving hazmat, instead they would shift the risk from one jurisdiction to another. Rerouting can actually reduce safety because it involves increased mileage, additional yard handling and dwell time, and may involve use of lines that for a variety of reasons, are less suited to hazardous materials movement. Banning certain hazmat movements by rail over specified routes would put the government in a position of assigning the risk of hazmat-related incidents and then shifting hazardous material transport from one location to another.

An alternative approach which railroads support, is to increase efforts aimed at finding and utilizing safer substitutes for the most toxic hazardous materials. These constitute a fraction of the hazardous materials moved by rail but, are responsible for approximately half of the overall cost of railroad insurance rates. The railroad industry is acutely aware of the magnitude of this challenge and that is why we reacted swiftly to the events of September 11th, hiring outside experts to work with us to develop a comprehensive security plan.

The plan includes an inventory of critical assets and has as its foundation a risk-based analysis of potential vulnerabilities. It includes a variety of countermeasures that are keyed to specific threat levels. The security processes and analysis detailed in the plan are periodically evaluated for effectiveness and modified as appropriate.

Because the U.S. rail network is vast, more that 140,000 route miles and open, our plan relies very heavily on access to intelligence information and we are in constant communication with intelligence and security personnel. I've testified here in the past about our plan so, I will not repeat anything further here. Let me just move quickly to what we believe should be included in any new rail security legislation.

We believe it is appropriate for the AAR Security Plan to serve as the basis for a government rail security plan because we have already identified the most important rail assets and the biggest threats to those assets. Any new legislation should also include adequate funding to implement anti-terrorism programs including funds to safeguard tunnels used by Amtrak and commuter railroads in the Northeast. We believe that funds should be appropriated to research and deploy rail security technologies including automated security inspections, infrastructure integrity monitoring, communication-based training control systems and reductions in tank car vulnerability.

Railroad police officers should be authorized to exercise law enforcement powers on any railroad, not just their own. To date, railroads have underwritten the cost of security measures to benefit the general public and national defense. But, protective measures required at the highest alert levels cannot be sustained by railroads alone. The industry security plan calls for use of the National Guard and local police to augment protection of critical infrastructure. States should be reimbursed by the Federal Government in those instances. Congress should also extend the Terrorism Risk Insurance Act to provide stability and certainty. Freight railroads are proud of the efforts we have taken to keep our Nation's vital rail transportation link open and secure since the terrorist attacks of September 11. We will continue to work with this Committee, others in Congress, the various Federal agencies and relevant parties to further enhance the safety and security of the Nation's railroads.

[The prepared statement of Mr. Hamberger follows:]

PREPARED STATEMENT OF EDWARD R. HAMBERGER, PRESIDENT/CEO, ASSOCIATION OF AMERICAN RAILROADS

On behalf of the members of the Association of American Railroads (AAR), thank you for the opportunity to meet with you today to discuss railroad security. AAR members account for the vast majority of rail mileage, employees, and revenue in Canada, Mexico, and the United States.

Our Nation's freight railroad industry, which has developed a comprehensive approach to protecting our rail network against terrorist threats, is keenly aware of the tension between the need for transportation efficiency and the assurance that our transportation systems are adequately protected from terrorist and other threats. We urge Congress to strike a proper balance between protecting our country's transportation assets and its citizens, and providing for the free flow of goods and promoting our international competitiveness. As Secretary Mineta has remarked, "What we don't want is for our checkpoints to become chokepoints.

Below I will discuss the many ways that U.S. freight railroads have addressed security in the post 9/11 era and how security efforts can be improved. I will also discuss pending proposals regarding railroad security from the perspective of freight railroads.

The Immediate Aftermath of September 11

The rail industry reacted swiftly to the events of September 11, 2001. In the immediate aftermath of the attacks, railroads tightened security and intensified inspections across their systems. Major railroads—which maintain their own police forces to help ensure the security of employees, property, and freight—put into place more than 50 permanent security-related countermeasures.

In late September 2001, the AAR Board of Directors established a Railroad Security Task Force. The task force had the full participation of AAR members, including our Canadian and Mexican members and the American Short Line and Regional Railroad Association. The overarching goals of this task force were (1) to ensure the safety of rail employees and the communities in which railroads operate; (2) to protect the viability of national and regional economic activity; and (3) to make certain that railroads can continue to play their vital role in support of our Nation's military.

Over the next several months, the task force conducted a comprehensive risk analysis of the freight railroad industry. Using CIA and national intelligence community "best practices," five critical action teams (consisting of more than 150 experienced railroad, customer, and intelligence personnel) examined and prioritized railroad assets, vulnerabilities, and threats. The critical action teams were:

1. *Information Technology and Communications:* This team examined the security of railroad communications, control systems, and information systems, including an evaluation of procedures regarding system redundancy, data confidentiality, emergency incident handling, and reconstitution of service.

2. *Physical Infrastructure:* This team assessed the physical security of essential bridges, buildings, dispatch centers, tunnels, storage facilities, and other structures, and created a database of critical assets. The team also addressed cross-border and port "gateway" physical security issues.

3. *Operational Security:* This team documented the "life cycle of a train and determined ways to minimize exposure to unplanned occurrences while trains are in operation. It also addressed fuel supply.

4. *Hazardous Materials:* This team examined the transport of hazardous materials by rail, with emphasis on materials that pose the greatest potential safety risk, such as poisonous gases.

5. *Military Liaison:* This team worked with the Department of Defense and its Military Traffic Management Command (MTMC) to determine immediate and ongoing military traffic needs. The MTMC, which has since been renamed the "Surface Deployment and Distribution Command, has designated 30,000 miles of rail corridors known as the Strategic Rail Corridor Network (STRACNET)—as essential to national defense.

In addition to the above activities, freight railroads cooperated fully with a separate team that covered passenger railroad security and involved the Federal Railroad Administration (FRA), commuter railroads, and Amtrak.

The Terrorism Risk Analysis and Security Management Plan

The end result of the work of the critical action teams was the development of a Terrorism Risk Analysis and Security Management Plan ("Plan"), a comprehensive, priority-based blueprint of actions designed to enhance the security of our Nation's freight rail network and its ability to support our economy, national defense, and public health.

The AAR Board of Directors adopted the Plan on December 6, 2001, and it remains in effect today. The security processes and analyses detailed in the Plan, including actions and countermeasures, are periodically evaluated for effectiveness and modified as appropriate—to ensure maximum efficiencies from advances in security technology and procedures.

The Plan defines four security alert levels and details the actions to be taken at each level as the terrorist threat increases.

Alert Level 1 is "New Normal Day-to-Day Operations" and exists when a general threat of possible terrorist activity exists but warrants only a routine security posture. Actions in effect at this level include conducting security training and awareness activities; restricting certain information to a need-to-know basis; restricting the ability of unauthenticated persons to trace certain sensitive materials; and periodically testing that security systems are operating as intended.

Alert Level 2 is "Heightened Security Awareness." It applies when there is a general non-specific threat of possible terrorist activity involving railroad personnel and facilities. Additional actions in effect at this level include security and awareness briefings as part of daily job briefings; conducting content inspections of cars and containers for cause; conducting spot content inspections of motor vehicles on railroad property; and increasing security at designated facilities.

Alert Level 3 means there is "a credible threat of an attack on the United States or railroad industry." A decision to declare Level 3 will be evaluated in light of the specificity of threat against railroad personnel and facilities. Examples of Level 3 actions include further restricting physical access and increasing security vigilance at control centers, communications hubs, and other designated facilities, and requesting National Guard security for critical assets.

Alert Level 4 applies when a confirmed threat against the rail industry exists, an attack against a railroad has occurred, an attack in the United States causing mass casualties has occurred, or other imminent actions create grave concerns about the safety of rail operations. Security actions taken at this level include stopping non-mission-essential contract services with access to critical facilities and systems; increasing vigilance and scrutiny of railcars and equipment during mechanical inspections to look for unusual items; and continuous guard presence at designated facilities and structures.

Alert Levels 3 and 4 can be declared industry-wide for a short period of time or can be declared in a particular geographic or operational area (e.g., the Midwest or hazardous materials) where or when intelligence has identified that terrorist action against a specific location or operation is imminent.

The Railway Alert Network and ST–ISAC

To help ensure that the parties involved have access to pertinent intelligence and other information, the rail industry is in constant communication with intelligence and security personnel at the Transportation Security Administration (TSA) and elsewhere in the Department of Homeland Security (DHS), the Department of Defense, the Department of Transportation (DOT), the FBI's National Joint Terrorism Task Force (NJTTF), state and local law enforcement, and others. A railroad police officer and knowledgeable railroad analysts work literally side-by-side with government intelligence analysts at NJTTF and within DHS to help evaluate intelligence at the Top Secret level.

The heart of this communication system is the Railway Alert Network (RAN). The major purpose of the RAN is to monitor the level of threat to the rail industry and to alert the industry if it changes. The hub of the RAN is AAR's Operations Center, which operates at the Secret level and is staffed with mobile communications around the clock at Alert Level 2 and is physically staffed at Alert Levels 3 and 4.

The RAN is linked to the Surface Transportation Information Sharing and Analysis Center (ST–ISAC). The ST–ISAC, which was created by the AAR at the request of the U.S. DOT, provides a robust capability for collecting, analyzing, and distributing security information from worldwide resources to protect vital physical assets and information technology systems. AAR-member freight railroads and Amtrak are members of the ST–ISAC. Cleared at the Top Secret level, the ST–ISAC also operates 24-hours-a-day, 7-days-a-week.

In addition, approximately 75 transit and commuter rail authorities (through APTA, the American Public Transit Association) have been members of the ST–ISAC. However, Federal funding for ST–ISAC membership for public transit agencies was discontinued by DHS. APTA recently asked TSA to consider restoring those funds. AAR supports APTA's request and, at the same time, asks that TSA also consider providing funds necessary to expand the reach of the ST–ISAC to all freight and commuter railroads that are not members of AAR.

As all of these efforts make clear, the rail industry strongly concurs with the July 2004 *Final Report of the National Commission on Terrorist Attacks Upon the United States* which called for "a different way of organizing government" that emphasizes a unity of effort as reflected in the phrase "one fight, one team." The Commission called for "unifying the many participants in the counterterrorism effort and their knowledge in a network-based information sharing system that transcends traditional government boundaries." Toward this end, we are working cooperatively with TSA leadership on operational and policy issues that will further enhance rail security.

Obviously, rail security efforts depend a great deal on the efforts of railroads' dedicated and highly professional employees—including engineers and conductors aboard trains, maintenance of way crews and inspectors working along the tracks, railroad police officers, and others. They are the "eyes and ears" in the industry's security effort, and we should all be grateful for their vigilance and care.

In recognition of the thoroughness of the railroad security plan and the dedication with which it has been put into effect, in June 2003 the Association of American Railroads was named a recipient of the U.S. Department of Defense's James S. Cogswell Award for Industrial Security. The Cogswell Award is the most prestigious award in the industrial security field. Of nearly 11,000 cleared contractors, only 15 were selected to receive the award in 2003. The railroad industry is also one of the few private sector industries to receive an "A" for its security efforts in an independent analysis by *The Washington Post*.

Notwithstanding all of these rail industry efforts, there can be no 100 percent guarantee against terrorist assaults. If such an assault involving freight railroads occurs, railroads have established programs and procedures that can and will be invoked that are designed to respond to, mitigate, and minimize the impact of such incidents. The programs and procedures include the establishment of emergency response plans for hazardous materials incidents, business continuity plans, and the training of rail employees and public emergency response personnel.

As previously mentioned, the freight rail industry works cooperatively with the Federal Government in efforts to enhance security. However, there are some areas where better coordination is needed. These improvements should focus on unifying government policy regarding freight rail security and more effectively coordinating the many governmental projects that affect rail security. In addition, the current system of dissemination of counter-terrorism information could be improved. The railroads' security plan is risk-based—the industry cannot protect everything all the time. Therefore, the government must provide timely and actionable threat information to enable efficient and effective deployment of limited resources.

Hazardous Materials Movements by Rail

Approximately 1.7 million carloads of hazardous materials (hazmat) are transported by rail throughout the United States each year—meaning that thousands of hazmat carloads are in transit by rail every day—and 99.998 percent of these shipments reach their destination without a release caused by an accident. Moreover, railroads have reduced overall hazmat accident rates by 90 percent since 1980 and by 49 percent since 1990.

In 2003 (the most recent year available), hazardous materials of all types accounted for 4.9 percent of total U.S. freight rail carloads, 5.4 percent of tonnage, and 6.3 percent of ton-miles. Tank cars transport approximately 68 percent of rail hazmat, 28 percent travel on intermodal flat cars, and the remainder moves in covered hoppers, gondolas, and other car types. The most potentially hazardous materials, termed toxic inhalation hazards (TIH), are a subset of these and nearly all are transported in tank cars.

No one disputes that efforts should be made to increase hazmat safety and security where practical. Railroads understand this better than anyone: because of their common carrier obligation, railroads are required by law to transport these shipments, even though this transportation involves extraordinary risks for the industry. This is one reason why railroads support the extension of the Terrorism Risk Insurance Act (TRIA) before it expires at the end of 2005. Even with TRIA, insurance has become more expensive and difficult for railroads to obtain, and it is not possible to fully insure against a truly catastrophic incident. Even though TIH accounts for a fraction of rail carloads, it contributes approximately 50 percent to the overall cost of railroad insurance rates. Insurance rates for AAR members have doubled this year alone. For these reasons, the transport of certain hazardous materials has the potential to be a "bet the business" activity for railroads. This leads to our recommendation that Congress should consider limiting railroads' liability for carrying out this public service, perhaps modeled after the Price-Anderson Act.

Freight railroads are constantly working to ensure the continued safety of hazmat transport.

- The industry operates under its comprehensive Terrorism Risk Analysis and Security Management Plan, as described earlier.
- Railroads assist communities in developing and evaluating emergency response plans; through their own efforts and the Transportation Community Awareness and Emergency Response Program (TRANSCAER) provide training for more than 20,000 emergency responders per year; and support Operation Respond, a nonprofit institute that develops technological tools and training for emergency response professionals.
- Trains containing specific amounts of the most hazardous materials are subject to special speed limits, passing restrictions, and inspections. Railroads increase track inspections, training, and installations of wheel defect detectors on routes over which these trains operate.
- Railroads work closely with chemical manufacturers in the Chemical Transportation Emergency Center (Chemtrec), a 24/7 resource that coordinates and communicates a broad range of critical information that may be needed by emergency responders in mitigating a hazardous material related incident.
- Upon request, railroads provide local emergency response agencies with, at a minimum, a list of the top 25 hazardous materials transported through their communities. The list assists local emergency responders in prioritizing their emergency response plans to what is most likely to be transported through their areas.
- Railroads participate in a variety of R&D efforts to enhance tank car and hazmat safety. For example, railroads, tank car builders, and car owners jointly fund the Tank Car Safety Research and Test Project (Project), which carefully analyzes accidents involving tank cars and continually updates a comprehensive database on the precise nature of damage to tank cars. Analysis of these data improves safety by improving researchers' ability to identify the causes of tank

car releases and help prevent future occurrences. The database is often cited by the DOT as a role model for other modes of transportation.

In addition to data gathering and analysis, the Project is engaged in numerous ongoing research efforts, including developing better steels for tank cars; measuring the railroad operating environment to refine tank car design requirements; investigating the forces generated in accidents to better understand ways to further improve tank car damage resistance; determining the effects of thermal protection degradation of rail tank cars in service; and providing validation and input data for a model used to evaluate the effects of fire on tank cars.

- Beyond the Project, the rail industry and rail suppliers are constantly investigating other ways to enhance tank car safety. For example, the AAR's Tank Car Committee (a group of technical representatives from railroads, shippers, and tank car builders/lessors that works closely with the FRA to, among other things, establish detailed tank car design standards and review individual tank car design drawings) recently supported a proposed new design for a chlorine tank car that would reduce the risk of a rupture while also reducing the number of shipments. Railroads are also working to determine what standards should apply to the next generation of tank cars that handle TIH.
- Freight railroads support the tank car vulnerability studies contained in the recently-passed SAFETEA–LU legislation and the requirement that the FRA initiate a rulemaking on tank car design, and we urge the FRA to meet the deadlines for these important projects.
- Railroads are working with TSA and independently to identify opportunities to reduce exposure to terrorism in high threat rail corridors and terminals.
- Railroads comply with DOT rule HM–232.

Despite rail efforts to ensure the safety of hazmat transport, a number of local and Federal proposals have been offered that would restrict rail movements of hazardous materials in one way or another. One such proposal would give state or local authorities the ability to ban the movement of hazmat through their jurisdictions. Another proposal would order railroads to provide local authorities advance notification of hazmat movements through their jurisdictions. Still another proposal mandates that hazmat routing decisions must be made by the Federal Government, rather than by railroads themselves.

The stated rationale for these types of proposals is often "protection" against terrorist attack (especially in perceived "high threat" areas) or a desire to be able to react more quickly to hazmat-related incidents, should they occur. The proposals may be well intended, but the end result of their enactment would likely be an increase in exposure to hazmat release and *reduced* safety and security.

Banning Hazmat Movements by Rail

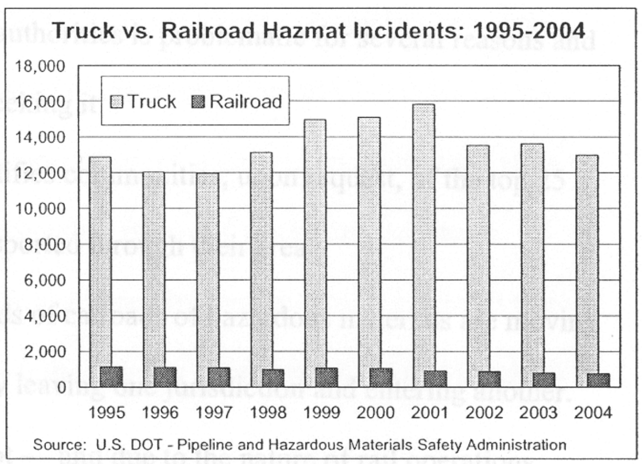
Banning hazmat movements in particular jurisdictions would not eliminate risks, but instead would simply shift them from one place to another. In shifting that risk, it could foreclose transportation routes that are optimal in terms of overall safety, security, and efficiency. For example, the rail network is not similar to the highway network where there are myriad alternate routes. In the rail industry, rerouting could add hundreds of miles and several days to a hazmat shipment, and those additional miles and days could be on rail infrastructure that is less suitable (for a variety of reasons) to handling hazmat. (In fact, CSX has determined that rerouting hazmat traffic away from Washington, D.C., as proposed by the D.C. City Council, would result in some 2 million additional car-miles per year the hazmat would have to travel.) Emergency responders along alternate routes may lack requisite expertise in handling the most dangerous commodities. Additional switching and handling of cars carrying hazmat could be needed, as could additional dwell time in yards. As the Department of Justice and the DHS noted in a joint brief opposing the D.C. hazmat ban, the increase in the total miles over which hazmat travels and the increase in total time the materials are in transit would "increase their exposure to possible terrorist action," and therefore potentially *reduce* safety and security. The U.S. DOT also submitted a statement recognizing that banning hazmat shipments through certain areas reduces both safety and security. Moreover, the costs to manufacturers and consumers of products that incorporate hazardous materials in their production would rise commensurate with the additional costs to transport these commodities.

If hazmat transport were restricted in one jurisdiction (either by Federal or local action), other jurisdictions would undoubtedly want to follow suit. In fact, that is already happening. In the wake of action (so far unsuccessful) by the D.C. City

Council to ban hazmat movements through Washington, similar efforts are being discussed in Atlanta, Baltimore, Boston, Cleveland, Chicago, Philadelphia, Pittsburgh, and probably other cities too, as well as the entire State of California. Banning hazmat shipments in even one city would be problematic; banning them in cities throughout the country would cause immense confusion and economic disruption nationwide—and would virtually shut down hazmat shipments by rail in this country.

Moreover, banning hazmat movements by rail would likely lead to many more movements by truck, but there is a much greater chance of release due to an accident when hazmat is carried by truck than when it is carried by rail. Railroads and trucks generate roughly equal hazmat ton-mileage, but trucks have 16 times more hazmat releases than railroads.

An integrated, effective national rail network requires uniform standards that apply nationwide. This uniformity, and the clarity and efficiency it brings, would be lost if different localities and routes were subject to widely different rules and standards or if local and/or state governments could dictate what types of freight could pass through their jurisdictions. The problem is especially acute for railroads, whose network characteristics and limited routing options mean that disruptions in one area can have profound impacts hundreds or even thousands of miles away. These disruptions negatively affect all rail traffic, not just hazmat traffic.



Banning certain hazmat movements by rail over specified routes would put the government in the position of assigning the risk of hazmat-related incidents, and then shifting hazmat transport from locations with higher assigned risk to locations with lower assigned risks. An alternative approach, which railroads support, is to increase efforts aimed at finding and utilizing safer substitutes for TIH hazardous shipments.

Hazmat Prenotification

Hazmat pre-notification to local authorities is problematic for several reasons and may not accomplish the goals of those seeking it.

First, the rail industry already notifies communities, upon request, of the top 25 hazardous commodities likely to be transported through their area.

Second, at any one time, thousands of carloads of hazardous materials are moving by rail throughout the country, constantly leaving one jurisdiction and entering another. The vast majority of these carloads do not—and due to the nature of rail operations, cannot be made to—follow a rigid, predetermined schedule. The sheer quantity and transitory nature of these movements would make a workable pre-notification system extremely difficult and costly to implement, for railroads and local officials alike. That's why the Fire Chief of Rialto, California, commented, "You'd have to have an army of people to stay current on what's coming through. I think it wouldn't be *almost* overwhelming. It would *be* overwhelming." The greater the number of persons to be notified, the greater the difficulty and cost would be.

Third, by definition, prenotification would vastly increase the accessibility of hazmat location information. Making this information far more accessible than it currently is could actually increase vulnerability to terrorist attack, not decrease it, because it would magnify the possibility that the information could fall into the wrong hands.

Fourth, railroads provide comprehensive training for hazmat emergency responders in many of the communities they serve, and they already have well-established, effective procedures in place to assist local authorities in the event of hazmat incidents. In fact, through the Transportation Community Awareness and Emergency Response Program, railroads help train more than 20,000 local emergency responders per year.

Finally, since railroads already make communities aware of what types of hazardous materials are likely to be transported through their area and since they already provide 24/7 assistance for emergency responders (many of whom railroads have trained), it is not at all clear that information obtained by local authorities through a prenotification system would actually improve their ability to respond to hazmat incidents in any meaningful way.

Railroad Security Legislation

A number of proposals have been offered in the Senate and House of Representatives regarding railroad security. Freight railroads are always ready and willing to discuss how security can be enhanced more effectively. To that end, we support the following provisions of rail security legislation:

- A comprehensive security plan should be developed that includes the identification of the most important rail assets and the identification of the biggest threats to those assets. In developing this plan, the government should use the AAR's Security Plan as the basis. Certain provisions of S. 1052, the "Transportation Security Improvement Act of 2005" and S. 1379, the "Rail Security Act of 2005," are consistent with this approach.
- Adequate funding to implement antiterrorism programs for passenger and freight railroads should be appropriated, including funding to safeguard tunnels used by Amtrak and commuter railroads in the Northeast. S. 1052 and S. 1379 each authorize more than $1 billion for grants for these purposes. Freight railroads should be able to apply for the grants directly rather than have to go through the states.
- Funds should also be granted to research and deploy rail security technologies, including automated security inspections, infrastructure integrity monitoring systems, emergency bridge repair and replacement, communication-based train control systems, and tank car vulnerability reductions. S. 1052 and S. 1379 authorize funds for these purposes.
- Railroad police officers should be authorized to exercise law enforcement powers on any railroad. This provision is in S. 1052 and S. 1379.

Railroads respectfully suggest that additional provisions would enhance rail security legislation:

- To date, railroads have been underwriting the cost of security measures for the benefit of the general public and for national defense. However, protective measures required at the highest alert levels cannot be sustained by the rail industry alone. This is reflected in the railroads' Terrorism Risk Analysis and Security Management Plan, which, at the highest alert levels, calls for the use of National Guard and local law enforcement support to augment industry protection of critical infrastructure. States should be reimbursed by the Federal Government for expenses associated with helping to guard critical rail assets at high levels of alert.
- The TSA and the FRA should clarify which agency has ultimate responsibility for which aspects of rail safety and security. Today, the allocation of responsibility is not always clear.
- A Federal grant program should be established to reimburse railroads for expenses mandated by the TSA or by other government entities, including mandates that result from high-risk corridor assessments.
- As noted previously, Congress should extend TRIA before it expires at the end of 2005. The need for a Federal backstop that provides stability and certainty remains.
- Congress should endorse the rail and chemical industries' request for a narrowly-tailored relaxation of antitrust prohibitions that would allow chemical companies and railroads to work together to reduce the public's exposure to IH shipments.

Finally, railroads believe that certain provisions of rail security legislation, including the following, are not necessary or appropriate.

- Banning hazmat transport by rail through certain jurisdictions or requiring prenotification (as called for, for example, by S. 1256, the "Hazardous Materials Vulnerability Reduction Act of 2005") should be opposed. Earlier in this testimony I explained why railroads oppose this legislation.

  On a somewhat related note, S. 1052 calls for DHS to approve railroads' "high hazard security threat mitigation" plans, "including alternative routing and temporary shipment suspension options." Routing of hazmat by railroad dispatchers is based on dynamic factors such as the condition of track, weather, and traffic congestion so as to ensure the selection of the safest possible route at any given moment. As the rail industry's response to Hurricane Katrina and Hurricane Rita makes clear, the industry is capable of quickly detouring traffic as conditions warrant. The Federal Government is ill-suited to perform this task, so the requirement for DHS approval of these plans should be dropped.
- Mandating that freight railroads submit employee security plans to DHS or DOT for approval, as called for in S. 1052 and S. 1379, is unnecessary.

  Since the terrorist attacks on September 11, 2001, freight railroads have provided ongoing general security awareness training to all employees, and some railroads have gone so far as to include security training as part of the annual FRA-mandated employee certification process. In an effort to further increase the level of security awareness for their employees, AAR member railroads are working with the National Transit Institute (NTI) at Rutgers University to develop a uniform security awareness curriculum that will significantly enhance the level of employee security training. The curriculum is modeled after the program NTI and the Federal Transit Administration developed for public transit agency employees.

  The goal of the training is to provide rail employees with an understanding of their role and responsibility in system security, and how to implement their companies' procedures upon detection of suspicious objects or activities. Course modules include instructions on reacting to threats, identifying suspicious activity, identifying suspicious objects, and responding to incidents.
- Mandates regarding the use of wireless terrestrial or satellite communication technology to track and locate rail cars carrying hazmat or to identify actual or imminent hazardous material release are premature. While railroads agree that there is benefit to the ability to detect hazmat breaches from rail cars and to communicate breach events to train crews and dispatchers, this technology must be carefully developed to ensure full functionality, appropriate design, reliability, and security. AAR is working with DHS and FRA to that end.

Passenger Railroads

As Members of this Committee are aware, more than 90 percent of the route mileage over which Amtrak operates, as well as a significant portion of the trackage over which many commuter railroads operate, is actually owned and maintained by freight railroads. Therefore, actions taken by freight railroads to enhance security also benefit passenger rail. Freight railroad police coordinate with and support Amtrak police to, among other things, increase uniformed police presence in rail passenger stations. Amtrak, commuter rail and transit authorities, and the freight railroads receive and share threat and incident information through the RAN and the ST-ISAC.

That said, freight railroad security-related plans and procedures are not specifically designed to protect passengers or to be a substitute for actions that Amtrak or other passenger railroad operators might choose or be requested to take.

Port and Border Security

The issue of port and border security extends far beyond the issue of rail security, although railroads, by virtue of the fact that they carry millions of containers unloaded from or loaded on to steamships each year and move hundreds of thousands of railcars and intermodal units across the Canadian or Mexican borders each year, are certainly impacted.

Ports have spent hundreds of millions of dollars enhancing their security, much of it funded by Federal grants. Railroads work closely with the Captains of Ports to ensure compliance with Coast Guard regulations regarding port facility security.

U.S. freight railroads also work diligently with the U.S. Bureau of Customs and Border Protection (CBP) and others to enhance border security. For example, a couple of years ago the U.S. and Canadian customs agencies and Canada's two major railways signed a declaration of principles to enhance security at the Canada-U.S.

border and to ensure secure rail access to the United States. The declaration—signed by the CBP, the Canada Customs and Revenue Agency (CCRA), Canadian National Railway (CN), and Canadian Pacific Railway (CP)—outlines principles for targeting, screening, and examining rail shipments transported by the Canadian carriers into the United States. The declaration includes guidelines for the electronic transmission of cargo information by the railroads to customs officials in advance of each train's arrival at the border and installation of Vehicle and Cargo Inspection System (VACIS) and radiation detection equipment at CN and CP border crossings.

Rail VACIS systems, which are also in use at rail border crossings with Mexico, use gamma ray technology to scan entire trains one railcar at a time. The gamma ray source and detectors are stationary as the train moves through the system. Inspectors examine scanned images of rail cars for contraband, potential terrorists, or terrorist weapons without opening them and potentially endangering lives. Suspicious rail cars are segregated for inspection, with minimal disruption to the flow of legitimate commerce. Today, where CBP has installed this equipment on the borders with both Canada and Mexico, 100 percent of rail cars are screened.

U.S. freight railroads are also active participants in the Customs-Trade Partnership Against Terrorism (C–TPAT), a joint government-business initiative within the CBP to build cooperative relationships that strengthen overall supply chain and border security. Through this initiative, CBP is asking businesses—including railroads—to ensure the integrity of their security practices and communicate their security guidelines to their business partners within the supply chain. I am happy to report that all U.S. Class I railroads are currently C–TPAT certified. The certification process involves a comprehensive review of a railroad's procedural security, physical security, personnel security, education and training, access controls, manifest procedures, and conveyance security.

Railroads have also been active participants in the significant expansion of Integrated Border Enforcement Teams (IBET) across the U.S./Canada border. The mandate of these teams is to enhance border integrity and security by "identifying, investigating and interdicting persons and organizations that pose a threat to national security or engage in other organized crime activity."

Finally, on January 5, 2004, CBP regulations requiring all transportation modes to submit cargo information electronically before arriving at the U.S. border came into effect. The rail industry was an active participant in developing these regulations, and railroads are complying with this requirement.

Conclusion

U.S. freight railroads are proud of the success they achieved in keeping our Nation's vital rail transport link open following the September 11, 2001 terrorist attacks. Since then, railroads have taken many steps to increase the security of our Nation's rail network, including the development of a comprehensive security management plan that incorporates four progressively severe alert levels. We will continue to work with this Committee, others in Congress, Federal agencies, and all other relevant parties to further enhance the safety and security of our Nation's railroads and the communities they serve.

STATEMENT OF WILLIAM L. CROSBIE, SENIOR VICE PRESIDENT, OPERATIONS, AMTRAK

Mr. CROSBIE. Thank you Mr. Chairman and Members. I would like to thank this Committee for the opportunity to testify on passenger rail security and the steps Amtrak has taken to enhance security and safety for our passengers.

You are to be commended for organizing this hearing and for advancing legislation to increase funding for rail security. I applaud your efforts and leadership on this matter and the attention given to rail security in S. 1052. I say this because time is of the essence. None of us can afford to wait until another catastrophe occurs. Those who use our trains should have the confidence that every reasonable action to protect and secure their well-being and safety has been taken.

Despite the openness of our Nation's rail system and the challenges it brings, I believe we have taken long strides in making our facilities and trains more secure. For us, security has become one of the costs of doing business because we know the nature of the threats our Nation faces will be with us for a long time.

Today, let me briefly outline for you what we have learned from previous terrorist events both here and abroad, the steps we have taken to address the knowledge learned from these events, and what we have planned to do in the near future. As part of the testimony I have submitted for the record, I have explained what steps Amtrak has already taken in the wake of the terrorist attacks in Madrid and London.

What I would like to do today in the short time I have allotted is explain what additional measures we have identified in our Security Investment Plan and what we at Amtrak could do to enhance the safety of our passengers and employees if we had additional resources.

For us, one of the more significant recent occurrences has been our ability to receive Federal funding for rail security improvements through the Fiscal 2005 Homeland Security Appropriations bill under the Intercity Passenger Rail Security Grant Program. Prior to Fiscal 2005, the Corporation did not qualify for such grant programs because it did not meet the eligibility requirements of being a state or local transit agency. In addition to having a risk assessment of Amtrak's Northeast Corridor and Chicago hub area performed by Homeland Security through their contracted corporation, Amtrak will use $6.1 million in funds for a number of security priorities, including but not limited to: increasing the number of explosive detection canine teams. Purchasing new explosive-resistant trash cans, adding radiological detection and verification pagers, and implementing a new passenger awareness program.

The funding provided as part of the Homeland Security grant will go a long way and will be put to good use. In addition to hardening our assets and improving our technology, we are relying more and more on the improved intelligence-sharing initiatives among key domestic agencies that are geared toward improving security within the rail industry.

Coordination with Federal agencies and national law enforcement organizations is essential to thwarting future potential terrorist attacks. We also worked with international partners, particularly those in Spain and England who have direct experience in dealing with rail-related terrorism. From a planning perspective, Amtrak has recently modified its security investment plan and has identified $156 million in critical funding needs. This is a detailed plan that prioritizes and itemizes our most urgent projects.

Amtrak maintains several control centers that need to have redundancy and to have a secure location for these vital communication and control operations. This project would consolidate these activities into one building. I cannot emphasize enough how crucial this element of our plan is to the entire package of security proposals. Amtrak needs to upgrade security at our largest stations which typically handle hundreds of thousands of people per day. In addition to closed circuit television and physical security improvements, explosive detection devices and additional radiological pagers would be disseminated to our sworn personnel for use in major stations and other strategic stations along the Northeast Corridor.

Amtrak effectively tracks train movement over the tracks that the Corporation owns, mainly over the electrified Northeast Corridor. Throughout the rest of the country, however, the chief means of communications with trains is through radio and cell phone telecommunication systems. Such systems do not adequately address reliable train tracking, emergency response efforts and have failed during critical incidents.

Amtrak has identified the need to significantly upgrade its existing, antiquated GPS system and would like to have it integrated with Amtrak's central computer system to provide the exact location for each train. Thus, additional funding in this area is critical and badly needed.

Last, with regard to our ongoing fire/life safety program, there are numerous infrastructure projects funded by the existing $100 million tunnel life safety grant provided in the Fiscal 2002 Department of Defense and Emergency Supplemental Appropriations for Recovery and Response to the terrorist attacks on the United States of which $71 million has been expended. This work is ongoing and significant progress has been made.

Funding is being used to improve radio coverage, wayside communication and tunnel portal security to secure all tunnel access points and improve security for trains traveling through the major tunnels on the Northeast Corridor. The nature of improvements consists of physical and technology-based security improvements, such as closed circuit television, event activated alarm systems, high-security fencing and lighting, the strategic placement of vehicle barriers. In addition, this tunnel security portion of the plan would also include similar upgrades at the Washington, D.C. First Street Tunnel and the Baltimore tunnels. Fencing improvements in the area of the Baltimore tunnels has already begun and fencing improvements are scheduled throughout Amtrak's 5-year capital plan.

The bottom line is this, we have learned much through the recent tragedies and terrorist attacks against public transportation. We have done our best to identify and prioritize our needs and use of the scarce funds where they will have the most impact. As you and this Committee are all too aware, as much as we would like to, Amtrak is not in a position financially to allocate huge amounts of additional resources to security. We are engaged in a very costly but long over due capital reinvestment program to rebuild our plant and equipment and to bring infrastructure to a state of good repair.

At the same time, we have also allocated additional resources where feasible for security as well as the operational——

The CHAIRMAN. We limit people to 5 minutes. I would appreciate it if you could find a way to end your testimony.

Mr. CROSBIE. I'm just about finished, sir. These dollars only go so far and we need additional resources to enhance the security of our national system. I'd be happy to answer a few questions.

[The prepared statement of Mr. Crosbie follows:]

PREPARED STATEMENT OF WILLIAM L. CROSBIE, SENIOR VICE PRESIDENT, OPERATIONS, AMTRAK

Mr. Chairman and Members of the Senate Commerce, Science and Transportation Committee, I would like to thank this Committee for the opportunity to testify on passenger rail security and the steps Amtrak has taken to enhance security and safety for our passengers.

You are to be commended for organizing this hearing and for advancing legislation to increase funding for rail security. I applaud your efforts and leadership on this matter and the attention given to rail security in S. 1052. I say this because time is of the essence. None of us can afford to wait until another catastrophe occurs. Those who use our trains should have the confidence that every reasonable action to protect and secure their well-being and safety has been taken.

Despite the openness of our Nation's rail system and the challenges it brings, I believe we have taken long strides in making our facilities and trains more secure. For us, security has become one of the costs of doing business because we know the nature of the threats our Nation faces will be with us for a long time.

Today, let me briefly outline for you what we have learned from previous terrorist events both here and abroad, the steps we have taken to address the knowledge learned from these events, and what we have planned to do in the near future.

Amtrak Reactions to Events at Home and Abroad

After the terrorist attacks of September 11, 2001, followed by the Moscow, Madrid, and London tragedies, the landscape of Amtrak's law enforcement responsibilities and duties changed markedly. Amtrak Police now have to ensure that thorough terrorism-based vulnerability and threat assessments are conducted, that emergency response and evacuation plans have been formulated, implemented and tested, and that Amtrak develops security measures that address not only vandalism and other forms of street crime, but the potential for Madrid and London type attacks on our passengers and on our property.

Since September 11, the Amtrak Police and Security Department has established and reinforced the following security improvements:

- Instituted Passenger ID procedure for purchase of most tickets.
- Improved baggage weight restriction policies for carry-on and checked baggage.
- Created a baggage tagging requirement.
- Developed and instituted a Security Threat Level Response Plan that is tied to the Homeland Security Advisory System and requires a series of security measures be undertaken at each alert level.
- Added 12 explosive detection canine teams.
- Created a Security Information Center in which bulletins, updates and security messages are disseminated to employees.
- Purchased and deployed radiological gamma/neutron pagers at Amtrak's major stations to address radiological threats and coordinated alerts with local police agencies.
- Coordinated security counter-measure issues with transit and freight railroad counterparts.
- Commissioned blast vulnerability studies of the New York tunnels and major stations.
- Revised the five-year Capital Plan to include numerous security upgrades, including high security fencing, yard security improvements, and access control upgrades.

After the Madrid bombings, Amtrak again increased uniform patrols at stations and on platforms and checked baggage rooms in greater frequency as well as critical infrastructure. It also:

- Issued Security Handbooks to all employees.
- Made technological improvements to the Railphone system on trains so that 911 could be dialed and individuals directly connected to a 911 Operator.
- Created security focus groups made up of employees and passengers to ascertain if security measures and objectives were being properly performed.
- Obtained assistance from freight law enforcement agencies who patrolled some Amtrak stations.
- Held system-wide security conference calls for managers and directed them to engage employees on their role in security matters.

As Amtrak continued to review its security needs and vulnerabilities, it recognized the need to create a security consciousness for all employees at all levels and to have a clear chain of command. Last year the corporation created an executive-level position, the Vice President of Security. Alfred J. Broadbent, a former Metropolitan Police Department Assistant Chief, was appointed to this position on August 2, 2004. All police and security functions now report to Mr. Broadbent, who reports to me. An Executive Security Committee was also established and meets weekly with him to discuss security policy, procedures, operational and capital security planning as well as terrorist threat and intelligence information.

One of the first efforts undertaken by the Vice President of Security was the re-engineering of Amtrak's primary terrorist security plan, the Security Threat Level Response Plan. This plan now contains more meaningful and measurable countermeasures and it is closely coordinated with recently created Security Coordinating Committees that consist of management level officials across Amtrak's operating departments. Each Amtrak operating division has a Security Coordinating Committee that meets regularly with Police and Security Managers to ensure that basic security practices and steps are undertaken and completed. The countermeasures contained in the Threat Level Response Plan provide a coordination of efforts directed to specific threats and attempt to create some basis for a layered security system that would improve deterrence capabilities. Some of the countermeasures that would be drilled down and enforced by Amtrak Police personnel and the Security Coordinating Committees would be assurance that only necessary access points are kept open, that gates, doors and other barriers are locked and secured, and that rolling stock and locomotives are locked and secured while this equipment is in a yard and/or standing at a station. Since August of 2004, the Amtrak Police and Security Department has also developed and implemented the following programs:

- Tactical Intensive Patrols (TIPS)—Sworn Amtrak personnel patrol specific station areas and conduct checks of baggage with passengers, provide security tip information and establish uniform presence.
- Train Riding Patrols—Sworn Amtrak personnel have been riding trains in a greater degree of frequency, mostly on the busy NEC.
- Counter-terrorism training conducted by the Federal Law Enforcement Training Center (FLETC) has been scheduled for all sworn personnel and was completed in FY05.
- Amtrak Management, DHS and the National Transit Institute developed a Security Awareness Training Program for all employees. This training is underway and is scheduled for completion in December 2005.
- Amtrak Police and Security coordinate its security concerns and initiatives with its Federal partners: DHS, TSA, DOT, and FRA.

Access to Resources

For Amtrak, one of the more significant recent occurrences has been our ability to receive Federal funding for rail security improvements through the FY05 DHS Appropriations bill under the Intercity Passenger Rail Security Grant Program. Prior to FY05, the Corporation did not qualify for such grant programs because it did not meet the eligibility requirements of being a state or local transit agency. In addition to having a Risk Assessment of Amtrak's NEC and Chicago hub area performed by a DHS contracted corporation, Amtrak will use $6.3 million in funds to increase security at Amtrak by:

- Adding explosive detection canine teams.
- Purchasing new explosive resistant trash cans.
- Deploying PROTECT (chemical detection equipment) systems at major stations.
- Conducting a Pilot Program with the Transportation Security Working Group and DHS on next generation CCTV systems.
- Adding radiological detection and verification pagers and portals.
- Increasing tunnel protection.
- Implementing a new passenger awareness program.
- Conducting a major exercise in Washington, D.C.

We have also been involved in numerous initiatives with the agencies that are geared toward improving security within the rail industry. Highlighted below are some of these interactions:

- Improved intelligence gathering capabilities by working closely with Federal and State agencies and industry partners. Agencies include: DHS, TSA (Transportation Security Operations Center—TSOC), DOT (Office of Intelligence and Security—OIS), FRA (Surface Transportation-Information Sharing and Analysis Center—ST/ISAC), and the industry AAR (Railway Alert Network—RAN).

- Continued assignment of an Amtrak investigator to work with the FBI in the New York Joint Terrorism Task Force. Other investigators will be assigned to the National Capital Region, Chicago, and Long Beach, CA JTTFs in the near future.
- DHS/TSA sponsored two emergency response drills in which multiple Federal, State and local agencies participated. Drills were based on terrorist act scenarios.
- DHS/TSA has worked with Amtrak as a venue location for the Transportation Workers Identification Card (TWIC) program.
- DHS/TSA and ICE has worked with Amtrak and upgraded the delivery of international traveler information for border inspection travel improvements and counter-terrorism purposes.
- FRA/TSA has partnered with Amtrak and used "airport type" screening at Amtrak stations during National Security Sensitive Events (RNC and Inaugural Event).
- TSA is also doing clearances and working closely with Amtrak in improving passenger manifest information and in coordinating Amtrak's industrial security clearance program.

In addition to Amtrak's security programs with the above agencies, Amtrak has also received the expertise and help of the State of New York's National Guard. It has provided additional resources in the form of National Guard personnel to support uniform forces at Penn Station, New York.

Next Steps

Today, Amtrak Police and Security continue its efforts to improve the safety and security of Amtrak passengers, employees and patrons. In February of this year, it participated in a special meeting and debriefing with leaders of Spain's law enforcement and military agencies and Renfre, the Spanish Commuter line involved in the Madrid bombings. Police and Security managers attended a special briefing last week in relation to the London bombings and plan to have a meeting with British Transport Police later this year to receive a similar briefing and "lessons learned" update on these terrorist tragedies. The department is also in the midst of a reorganization that will channel and deploy resources in a more effective manner to address the security realities of today's rail systems.

From a planning perspective, Amtrak has recently modified its Security Investment Plan and has identified $156 million in critical funding needs.

- **Dispatch and Control Centers**—Amtrak maintains several control centers that need to have redundancy and to have a secure location for these vital communication and control operations. This project would consolidate Amtrak's CETC (Centralized Electrified Traffic Control Center), CNOC (Consolidated National Operations Center) and the NCC (Police Department Radio Center) into one building. This location would be constructed so that access is restricted and basic CPTED (Crime Prevention Through Environmental Design) concepts employed. I cannot emphasize enough how crucial this element of our plan is to the entire package of security proposals.
- **Securing Amtrak's Largest Stations**—Amtrak needs to upgrade security at the largest stations which typically handle hundreds of thousands of people per day. In addition to CCTV and physical security improvements, explosive detection devices and additional radiological devices/pagers would be disseminated to sworn personnel for use in major stations and other strategic stations along the NEC.
- **Amtrak Train Tracking, Communications and Critical Incident Response**—Amtrak effectively tracks train movement over the tracks that the Corporation owns, mainly over the electrified NEC. Throughout the rest of the country, however, the chief means of communications with trains is through radio and cell phone telecommunication systems. Such systems do not adequately address reliable train tracking, emergency response efforts and have failed during critical incidents. For example, Amtrak's radio system cannot be used where it does not own track and, therefore, Amtrak radio train communications is dependent upon the host railroad network. Cell phone technology can be limiting and is often dependent upon the footprint of the cell phone provider. Amtrak has also identified the need to significantly upgrade its existing,

antiquated GPS system (over 8 years old). The GPS system needs to be integrated with Amtrak's central computer system and CNOC to provide the exact location for each train on a minute-by-minute basis. Thus, additional funding in this area is critical and badly needed. Such upgrades and the introduction of satellite telephone communication systems would provide uninterrupted communications.

Fire/Life Safety

Last, with regard to our ongoing fire/life safety program, there are numerous infrastructure projects funded by the existing $100 million tunnel life safety grant provided in the FY02 Department of Defense and Emergency Supplemental Appropriations for Recovery and Response to terrorists attacks on the United States (Pub. L. 107–117) of which $71 million has been expended. This work is ongoing and significant progress has been made.

Funding is being used to improve radio coverage, wayside communication and tunnel portal security. Other components of this element are to secure all tunnel access points and improve security for trains traveling through this area of the NEC. The nature of improvements consists of physical and technology based security improvements, such as CCTV, event activated alarm systems, high security fencing and lighting, and the strategic placement of vehicle barriers. In addition, this tunnel security portion of the plan would also include similar upgrades at the Washington, D.C. First Street Tunnel and the Baltimore tunnels. Fencing improvements in the area of the Baltimore tunnels have already begun through the capital plan and fencing improvements are scheduled throughout Amtrak's five-year capital plan.

I hope that this overview has provided you with a better understanding of what Amtrak has done, and continues to do, to enhance safety for our employees and passengers. I will gladly respond to any follow up questions that you may have on rail security.

STATEMENT OF EDWARD WYTKIND, PRESIDENT, TRANSPORTATION TRADES DEPARTMENT, AFL–CIO

Mr. WYTKIND. Thank you Mr. Chairman for having this hearing. At the outset, I just want to say that we believe, on behalf of the employees in the rail industry, that rail security in this country and the actions of the Department of Homeland Security or I guess, inaction, have been sorely lacking. We've heard a lot from the railroads over the years and including this morning about action teams, task forces, countermeasures and a lot of good sounding initiatives. But, I must report that the workers in this industry and their unions haven't been enlisted as partners in these efforts.

Access control at key facilities and infrastructure is lacking and security training is basically non-existent. Workers are still being discouraged, if not intimidated, from reporting safety and security risks and Federal funding in our judgment hasn't kept pace with the needs of rail security in this country.

The workers that I have spoken to, inform me that they feel no safer or more prepared then they were before 9/11. They feel as if too many railroads are getting away with showing videos as a substitute for real training and they feel as if the rail network hasn't been adequately secured. These are the workers that work on the front lines. They don't just talk about working, they actually go to work every day and make the system as safe and secure as possible.

I want to thank you, Mr. Chairman and the Members of this Committee for your introduction of S. 1052. The rail title is especially comprehensive and will address a number of serious security issues in the rail system. We've heard from Mr. Hamberger about our workers being the eyes and the ears of the system but the railroad companies are failing to give these workers the tools they need to be those eyes and ears. Let me be clear, the workers are not receiving the training that you are hearing about today. I'm still puzzled by the TSA's testimony about all these front line workers being trained because they, themselves have been slow in moving security training initiatives. Our members at one of the freight carriers told us just a few days ago that they get a 14-minute video at best, maybe once a year. I've seen one of the videos and it does little to prepare workers. It offers vague and often very conflicting guidance and one video actually told the workers not to overreact but not to under-react. I'm just kind of wondering what that means. They don't know what a security risk is, they are being told to be vigilant but they have no idea what these so called "countermeasures" the railroads are putting into place mean and how they apply to their lives as workers.

Perhaps worst of all, the initiatives that the industry has instituted since 9/11 have had no involvement by the unions and their members in the rail industry. Front line workers are in a position to spot security risks. Every witness will tell you that, including those in the government. They are the first on the scene along with firefighters and police. We have come to the conclusion that the only way that the workers will be trained is for the government to be told that they will institute regulations and for the carriers to have to abide by those regulations. It's not enough for the railroads to pay experts to provide very nice Power Point presentations. If the workers are not getting the training done at the rank and file level then it doesn't make a difference. I'm here to tell you that four years after 9/11 it's not happening and we believe it's a disgrace.

I want to commend you Chairman Stevens, Senator Inouye and others for including Section 310 in the legislation which will bring real training to the workers. But, I must caution that oversight will be badly needed because the Department of Homeland Security has been badly delinquent in fulfilling Congressional mandates that this Committee instituted to force flight attendants training on the air carriers. The railroads have told you this morning that the training is unnecessary, they claim that they are working with the National Transit Institute to develop a program. They are missing the point. It doesn't matter how good the program is, we know NTI does a lot of good work in public transportation but the training curriculum is useless if it doesn't get down to the local level. My rail union leadership told me that they didn't even know about the NTI program that's being peddled this morning, until it arrived in the mail coincidentally this week, right before today's hearing.

I know that my comments conflict with Mr. Hamberger's, but they are based on personal assessments by workers and their union reps that know what the vulnerabilities are in the rail system. And we hope that the Committee will reject the industry's pleas to water down or eliminate these worker training requirements because the provisions in your bill will really make a huge down payment in that effort.

I'll summarize by saying that we think the system itself needs to be better secured as well. I've heard too many stories from too many local workers and union reps about locomotives being left with no one around, about the ability to waltz in and out of rail facilities and about the ability to trespass with really very little resistance from the railroads. And in regards to Amtrak, that's also a problem but I believe that Amtrak has a resource problem, I believe that Amtrak wants to try to deal with the security concerns but the workers are being left untrained. A lot of them aren't even credentialed and the resources that Amtrak is dedicating to security is just this tiny down payment for what the railroad actually needs.

So, I'm happy to work with this Committee to try to get a strong rail security bill passed but I think something needs to be understood. The railroads are not providing the training that is so urgently needed. The resources Amtrak is getting are not enough to deal with security and it's very important in my judgment that the Department of Homeland Security has to be held accountable for the lack of action and attention rail security has recorded. Thank you and I'm happy to answer any questions you have.

[The prepared statement of Mr. Wytkind follows:]

PREPARED STATEMENT OF EDWARD WYTKIND, PRESIDENT, TRANSPORTATION TRADES DEPARTMENT, AFL–CIO

Chairman Stevens, Co-Chairman Inouye, and Members of the Committee, on behalf of the 29 affiliated unions of the Transportation Trades Department, AFL–CIO (TTD), I want to thank you for giving transportation labor an opportunity to testify today on our priorities and strategies for enhancing rail security.[1]

This hearing occurs at an auspicious time. Having just observed the fourth anniversary of the September 11, 2001, terrorist attacks on America, we are reminded again that rail security measures—both in the transport of passengers and freight—have been sorely lacking. The brutal attacks in the passenger rail systems of London and Madrid served as the most recent wake-up call, but in reality we have long known that rail transportation is a tempting target for those that wish this Nation harm. Unfortunately, beyond vague warnings by the Administration, and promises of action by the rail industry, little has actually been done. Vulnerable rail targets have not been hardened, access control at key facilities is lacking, security training is basically non-existent, workers are still being discouraged from reporting safety and security concerns, and Federal funding has not kept up with the immediate security needs of this vital sector of our transportation system.

Last month, the new head of the Transportation Security Administration told a Senate committee that the state of transit security was, and I quote, "outstanding." Echoing this assessment, I am sure that freight rail industry representatives will trot out fancy reports and charts supporting their claims that much has been done to secure our rail transportation system. We will hear about "action teams," task forces, "countermeasures," daily security briefings, worker training and a whole host of wonderful initiatives. And we will hear about the industry's partnering activities with others in the private sector and government. Unfortunately, I must sadly report that workers and their unions have been left in the dark about these activities and the railroads have not enlisted their employees as partners in this endeavor. In fact, the workers I have spoken to inform me that they feel no safer or more prepared than they were before the September 11 attacks. This situation has gone on for too long and is simply unacceptable. We need to get serious about rail security and we need leadership from Congress to address the critical areas of concern that workers and other stakeholders have so readily identified.

On this point, I want to thank you Chairman Stevens, Senator Inouye, the Co-Chairman of the Committee, and the other Senators who have joined with you in introducing the Transportation Security Improvements Act of 2005 (S. 1052). While there are some changes we would like to see to this bill, the product you have offered is comprehensive and would address a number of security vulnerabilities across the various modes of transportation, including of course the rail sector.

[1] Attached at 1 is a complete list of TTD's affiliated unions.

When you remember the size and scope of our rail system and infrastructure, the lack of attention and focus on security is hard to understand or accept.[2] In addition, we must recognize that given the open nature of our rail transportation network, we are never going to be able to secure it entirely, since, unlike aviation, it simply is not housed in a relatively closed or contained infrastructure. Indeed, inter-city and commuter rail is designed to be accessible and at least part of its appeal is this relative ease of use.

Given these facts, it is absolutely imperative that we take the steps that can be implemented and that are compatible with a system that is so critical to our national economy. I will concede that we can't build a fence around every train track in America. But we can train workers and leverage technology to better monitor and control this vast infrastructure. We may not be able to screen every passenger at every station, but there is simply no reason, not one, that workers should be discouraged, or discriminated against, for speaking out on security.

Treating Employees as Partners

We need to start treating front-line employees as true partners in the effort to protect our rail system. These workers greet passengers, sell tickets, operate and staff the trains, maintain and inspect track and equipment, dispatch trains and fix cars. In short, they are in an excellent position to spot security risks and terrorist threats. And in the event that an attack does occur, our members will be on the scene and the first to respond along with firefighters and police.

Security Training

Let me be extremely clear about this point—despite the claims of some in industry, workers are not receiving meaningful security training. Our members at one freight carrier have told us that at best they get a 14 minute video—maybe once a year, but maybe not. And one local leader reported that new hires don't even get to see the movie. Mr. Chairman, I have seen this so-called training video and there's only one problem—it does virtually nothing to prepare a worker on how to address security problems. It offers vague and often conflicting guidance. My personal favorite is when it instructs workers, in dealing with a person on the property who is not supposed to be there, to not overreact, but also not to underreact. What does that mean? Workers still do not know what constitutes a security risk, though they are told to be "vigilant." They do not know how to respond when they do see someone or something suspicious and they certainly don't know what to do if something actually happens. I realize that my comments conflict with those of Mr. Hamberger. But I am offering my observation to this Committee based upon personal assessments by rank-and-file workers and local leaders who understand their railroad property and its vulnerabilities and know first-hand how little is being done to deal with security risks.

It is well known that real training is effective. We know this from positive experiences in the safety arena and experts confirm that it is even more crucial in security. Rafi Ron, former Director of Security at Tel-Aviv Ben-Gurion International Airport told a Senate committee last month that behavior pattern "techniques implemented by trained security and non-security personnel have proven to be a valuable measure in the detection and prevention of terrorist attacks in public faculties." Ron went on to observe "training provides the skills and confidence not only to law enforcement officers . . . but also to employees who are present at every point in the system. No one is in a better position to recognize irregularities on the ground than the people who regularly work there."

The Volpe Center recently concluded that "probably the most significant factor in determining whether a transportation employee makes a helpful or harmful decision during an emergency is training. Trained and alert transportation professionals can make the difference between success and disaster. Characteristics such as acting responsibly to protect the lives of the public; keeping one's cool and keeping passengers calm; contacting emergency assistance authorities quickly and reporting the essential details accurately; working cooperatively as a member (and sometimes a leader) of a team with a common goal—can all be enhanced through proper training."

These observations and conclusions are not surprising—it is quite frankly common sense that a robust and consistent training regime is a cost effective way to enhance

[2] There are over 100,000 miles of rail in the U.S.—22,000 of miles of it used by Amtrak in 46 states and the District of Columbia. In 2004, Amtrak served 25 million passengers, or approximately 68,000 a day. Commuter rail operations add approximately 978,000 passenger trips each weekday. The freight rail carriers carry 42 percent of our Nation's domestic intercity freight and in 2002 alone over 109 million tons of hazardous material.

rail security. Unfortunately, employers, under profit and operational pressures, too often short-change this critical security component. We have come to the conclusion that the only way workers are going to get the security training they need is for the Federal Government to come in and tell the carriers that they must offer this training because it is too important to ignore. It is not enough for the railroads to pay experts to develop nice reports unless the materials developed are delivered to the employees in the form of a comprehensive, mandatory training program. That is not happening today and we believe this is a disgrace.

On this point, I want to commend Chairman Stevens and Senator Inouye for including a provision (Section 310) in S. 1052 that would accomplish this objective. Specifically, Section 310 would require DHS, within 60 days of enactment, to develop and issue detailed guidance for a rail worker security training program. The guidance issued by DHS will require a training program that would encompass a number of appropriate elements including crew communications and coordination activities; evacuation procedures; use of protective devices; live situational training exercises and ways to determine the seriousness of any situation. Sixty days after DHS issues these guidelines, each rail carrier is required to develop a training program and submit it to DHS for review and approval. DHS may also require the rail carrier to make revisions to the training program that the Secretary considers necessary to ensure that the program meets the guidance requirements. The carrier will then have 180 days to complete the training of all front-line workers in accordance with the DHS approved program.

I have little doubt that some in industry will complain that this program is too burdensome and that they should be allowed to institute training on their schedule. I am also sure that some rail carriers will claim that since training is already being done, that this Committee should simply stand down and allow industry to proceed on its own. We hope you will reject those pleas for more inaction. As I have stated, we have talked to too many front-line workers who dispute the industry's claims to allow this fiction to perpetuate any longer. Comprehensive security training must be mandated, and it must be instituted as soon as possible. I applaud you Mr. Chairman and Senator Inouye for recognizing this fact and I urge the Committee to retain this provision as your bill moves through the legislative process.

Providing Whistleblower Protections

We must also ensure that workers who report or identify a security risk will not face retribution or retaliation from their employers. Simply put, a rail worker should not have to choose between doing the right thing on security and his or her job. Unfortunately, too often this is exactly what occurs.

Rail workers and their unions have long argued that despite the whistle-blower protections included in current law (49 U.S.C. § 20109), employees still experience employer harassment and intimidation when reporting accidents, injuries and other safety concerns. Indeed, in a Federal Railroad Administration (FRA) report issued in July 2002 entitled *An Examination of Railroad Yard Workers Safety* (RR02–01), the FRA conducted focus group interviews with certain groups of rail workers. The FRA stated, "Perhaps of most significance, rail labor painted a generally adversarial picture of the safety climate in the rail industry. They felt that harassment and intimidation were commonplace, and were used to pressure employees to not report an injury, to cut corners and to work faster."

Section 311 of S. 1052 does attempt to address this problem by providing certain whistleblower protections for workers who report security concerns. While this provision is a step in the right direction, and I want to thank Senator Lautenberg for working with us on this issue, it needs to be strengthened to provide workers with a fair and expedited process to seek redress in whistleblower situations. In addition, if we are ever going to stop discrimination against workers who report security problems, penalties and fines must be increased to create a real deterrent and not just make violations a cost of doing business.

I should note that as part of the Sarbanes-Oxley Act, Congress, on a bi-partisan basis, included whistle-blower protections for those who report shareholder fraud violations or violations of Securities and Exchange Commission rules. (*See*, 17 U.S.C. 1514A). Surely, if we can protect whistleblowers who report financial security problems, we can also protect those who report rail security concerns.

Everyday, rail carriers and the government ask front-line workers to be more vigilant about security risks and to report possible breaches. With the right training, rail workers are more than happy to play this role. But it is disingenuous to ask workers to report problems and at the same time refuse to provide the basic protections needed to ensure that such reporting will not result in employer retribution.

Securing Rail Facilities

Our members are also increasingly concerned that rail yards and facilities are largely open areas where people can come and go virtually unchallenged. In general, we need to ensure some type of security perimeter around yards and other sensitive facilities and better access control. Indeed, I would note that shortly after the Madrid attacks Amtrak issued a security notice reminding employees to wear their identification badges despite the fact that, according to reports from workers we have received, many employees have still not actually received their credentials. This of course raises the question of how access control is being achieved in those situations.

On a related issue, we need procedures and technology in place to better monitor and protect tracks, signals and switches. Given the amount of hazardous material that is moved by our rail system, it does not take a lot of imagination to see how a terrorist could sabotage key points in our infrastructure to create a deadly accident. Signal systems and track switches are too easy to manipulate and access to these systems must be better controlled.

When problems are spotted, our members are told to contact appropriate security personnel. The problem (besides the fact that there is no training or set procedures on who to contact) is that in many instances, especially in rural areas, security guards are often not on the property and many miles away. In fact, one rail worker stationed out West recently told me that the carrier had one security person to contact during emergencies covering a 1,000 mile territory. And yet we can't seem to convince our employers that front-line workers need training on what to do when there is a security threat and security personnel are not available to immediately respond.

In general, we are increasingly concerned with the lack of security with respect to the transport of hazardous materials. Tank car integrity standards are critical and out-of-date equipment must either be brought into compliance or retired. While not the work of terrorists, the tragic accident in Graniteville, South Carolina, where nine people died, 310 required medical attention and 5,400 residents were forced to evacuate, was a stark reminder of the consequences of a hazardous material release. And just last Saturday, two Union Pacific trains collided in Texarkana, Arkansas, releasing propylene and leading to a massive fire and explosion. Simply put, rail transportation is a dangerous business on a normal day. In the post-9/11 environment the challenge of protecting the Nation from terrorist threats directed at rail transportation multiplies.

Amtrak Security

Let me say a word about rail security as it relates specifically to Amtrak. It is no secret that every year Congress provides Amtrak just enough funding to limp through another fiscal crisis. In this environment, it is impossible for our Nation's national passenger carrier to invest the capitol resources needed to make major improvements to rail security. This starvation diet that we have put Amtrak on must end; not only because it represents bad transportation policy, but because it creates security issues and problems that are unacceptable. Again, on this point, let me note the leadership of Chairman Stevens, Chairman Lott, Senator Lautenberg and others who have pushed this Committee to approve a multi-year reauthorization bill and have led the fight in the annual appropriations process that is still ongoing as we speak.

Clearly, Amtrak needs stable, long-term resources to shore up its financial challenges. But in the context of security, we cannot expect Amtrak to fend for itself while we spend billions addressing so many other aspects of homeland security and the war on terrorism. We have always believed that transportation security is an integral element of our homeland security efforts and publicly supported transportation systems like Amtrak deserve adequate Federal resources to protect their passengers, workers and the public from terrorist threats.

There has also been a lot of talk, both from Amtrak and the Administration, about the need to contract-out as many Amtrak services as possible and to privatize parts or all of the system. Again, we have serious transportation policy reasons why these proposals should not be adopted and I will not expand on them at this hearing. But let me also point out that in-house employees are known quantities that in many cases have security responsibilities they must perform. If these functions are contracted-out, as they already are in some areas, it calls into question how these functions will be handled and makes it that much more difficult to reliably control access to train operations.

Final Thoughts

Achieving rail security is of course not a simple task. But we cannot allow this challenge to go unmet any longer. Four years after 9/11 and in the wake of deadly attacks in London and Madrid, our government and rail employers are still not doing enough to make rail transportation as secure as possible. Rail security needs and deserves attention and focus from policy makers. Carriers must be required to follow security procedures, employees must be trained and afforded whistle-blower protections, and rail yards, facilities, tracks, equipment and signal system must be secured. All of transportation labor has a vested interest in improving rail security and Mr. Chairman and Co-Chairman Inouye, TTD stands ready to work with you to achieve this common agenda.

Thank you again for giving TTD an opportunity to share our views today.

TTD AFFILIATES

The following labor organizations are members of and represented by the TTD:

- Air Line Pilots Association (ALPA)
- Amalgamated Transit Union (ATU)
- American Federation of State, County and Municipal Employees (AFSCME)
- American Federation of Teachers (AFT)
- Association of Flight Attendants-CWA (AFA–CWA)
- American Train Dispatchers Association (ATDA)
- Brotherhood of Railroad Signalmen (BRS)
- Communications Workers of America (CWA)
- International Association of Fire Fighters (IAFF)
- International Association of Machinists and Aerospace Workers (IAM)
- International Brotherhood of Boilermakers, Blacksmiths, Forgers and Helpers (IBB)
- International Brotherhood of Electrical Workers (IBEW)
- International Federation of Professional and Technical Engineers (IFPTE)
- International Longshoremen's Association (ILA)
- International Longshore and Warehouse Union (ILWU)
- International Organization of Masters, Mates & Pilots, ILA (MM&P)
- International Union of Operating Engineers (IUOE)
- Laborers' International Union of North America (LIUNA)
- Marine Engineers' Beneficial Association (MEBA)
- National Air Traffic Controllers Association (NATCA)
- National Association of Letter Carriers (NALC)
- National Federation of Public and Private Employees (NFOPAPE)
- Office and Professional Employees International Union (OPEIU)
- Professional Airways Systems Specialists (PASS)
- Sheet Metal Workers International Association (SMWIA)
- Transportation Communications International Union (TCU)
- Transport Workers Union of America (TWU)
- United Mine Workers of America (UMWA)
- United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union (USW)

The CHAIRMAN. Thank you very much, I would urge the gentlemen to be precise in your answers because we are limited on time.

Matter of fact, there's two amendments on the floor right now that affect my state and I'm anxious to get this hearing over. But, Mr. Hamberger, you've alluded to some confusion as to whose in charge, TSA or FRA, who do you think is in charge and who should be in charge?

Mr. HAMBERGER. I believe that TSA should be in charge of security, and FRA in charge of safety. The two, however, overlap. As you heard in the first panel, a tank car could involve a safety issue, it could also raise a security issue. So, I think there needs to be better coordination. I think Secretary Hawley and Mr. Boardman have undertaken that and have had a series of meetings. Within the Department of Homeland Security itself, however, there is still, and I think Mr. Hawley alluded to it this morning, there needs to be a single point of contact for the industry. We hear from the Information Analysis and Infrastructure Protection Group, from the Coast Guard, from TSA, from different organizations within DHS coming to our members and asking for oftentimes overlapping requests for data. There just needs to be a single point of contact. We've met with Secretary Hawley on that and I think he is moving in that direction.

The CHAIRMAN. Mr. Crosbie, I'm sure we're going to hear more about the needs of Amtrak, but has the Board explored increasing the cost to the passengers instead of totally requesting additional Federal money to meet the improvements you've mentioned?

Mr. CROSBIE. As I understand it, it was before my time at Amtrak, it was considered post 9/11 and there was a significant push back from some of the state governments on adding a security fee.

The CHAIRMAN. Well, I remember right after 9/11 going to Nome and finding TSA in the terminal there at the small airport. They had taken over a third of the terminal, which has been paid for by the state and the city. They were charging passengers more money to provide security. Why is it that rail transportation has not been willing to step up to the plate and ask the passengers to pay part of the security and safety costs?

Mr. CROSBIE. We, within Amtrak, we've certainly considered doing that and in the past when we had proposed, like I had said, there was a significant resistance to implementing that. We haven't ruled it out entirely, but based on the past response, we haven't considered it further.

The CHAIRMAN. Am I right that your number of passengers has increased since 9/11?

Mr. CROSBIE. Yes.

The CHAIRMAN. Substantially?

Mr. CROSBIE. Sorry, sir.

The CHAIRMAN. There's been a substantial increase?

Mr. CROSBIE. Substantial, yes, it has been.

The CHAIRMAN. Mr. Wytkind, I appreciate your comments about Senator Inouye's and my involvement in this bill and I understand what you're saying about training. One of the problems is, when I think of some of the airline unions, they've been very much involved in training themselves. Why haven't you?

Mr. WYTKIND. Well, actually they have been and that's actually a good example of the problem. In the hazardous materials area, the rail unions have had a very robust hazmat training program that actually receives some Federal support. But, when we've tried to approach the railroads to participate in that program and perhaps even help us finance it so that it has the support it needs, we've met a lot of resistance. And any attempts we've ever made to strengthen training for workers or to have them covered by certain safety regulations, we've always met with resistance from the railroads. Anytime safety re-authorization legislation has been pending in this Committee, we've met resistance from the railroads.

So, my message to you is, I think the rail unions have a strong track record of delivering training to their members under very limited resources. I would submit to you, that given the sheer size of the workforce in the country and the amount of responsibility that they bring every day to work, to the job, that they need the support to make sure they're prepared. When I hear local union reps tell me things like our members don't feel any more prepared today than they did 4 years ago, before 9/11, that brings chills down my spine and I'm sure to a lot of other people.

The CHAIRMAN. I don't know if you know, but I probably carried a union card longer than anyone in the room. But, as a practical matter, I understand that when your people are laid off they automatically continue to receive full pay. There's a real question about the retirement and layoff costs of labor in terms of these railroads, particularly Amtrak. What do you say about that?

Mr. WYTKIND. I don't think those issues are applicable to security in the sense that——

The CHAIRMAN. It takes money away from the system.

Mr. WYTKIND. Well, the Congress has affirmed and reaffirmed its very strong support for the railroad retirement system that the rail employees are covered by, including the railroads themselves that have always supported it. So, the costs on the system for retirement, to me, are unrelated to whether we should be training workers at the rank and file level.

The CHAIRMAN. Thank you very much. We'll go by the early bird rules so, we have Senator Lautenberg's, Senator Lautenberg, I have a call from the Co–Chairman, I'll be right back. Would you proceed?

Senator LAUTENBERG. [presiding] Thank you very much. The concerns that we have about rail security loom largely in front of us, and yet we hear—well, in one instance—that the private sector will provide it. And in response to a question I asked about oversight and providing the appropriate budget for rail security review by the Federal Government, we were told that—well, we have standby personnel, we have Air Marshals, we have people—they are going to be called upon long after the fire has begun. They can't suddenly switch from the Air Marshal population over to the railroads. The problem, Mr. Wytkind, is that we know that Amtrak is under funded to begin with. It is difficult to compare with the airline situation, with its repeated bankruptcies that we're called upon to bail them out of. Also, the infrastructure and operations that provide our great aviation service that we have in our country are largely supplied by the Federal Government, looking at much of the FAA and the other government services that are connected with aviation. Amtrak has never been able to get its head above water, because from the day that Amtrak became a corporation on its own being, we work with the same old equipment, we work with the same old systems, we work with a constantly reduced level of funding and once and for all, we're going to have to take a plunge. And that plunge is going to say that we are going to upgrade things, that we are going to buy cars that are better than 40- or 50-year old ones and locomotives as well and make the investment that so many other countries make.

And we see it, for instance, in Germany with maybe $7–10 billion dollars a year going into their system and if you take a ride on it, you'll know where it's going. The TGV in France will take you from Brussels to Paris at an hour and 20 minutes for a 200-mile ride. If we supply that kind of service here, we could reduce congestion in our aviation system that now has us late for appointments, et cetera. So, I think that we have some opportunities to take a realistic look at where we go here and I'm appreciative of the commentary that we've heard from our witness and I'm sorry that I wasn't here at an earlier point.

Mr. Wytkind, one of the things that we noticed is the substantial increase in violations of the Federal hazmat worker training laws and you talked extensively about that and I commend you for it. Now, I worked with the Committee to almost double the minimum civil penalty in law for these types of violations. You talked about how important hazmat training is to running a safe and secure railroad. What do you think we ought to do? Should the government take the responsibility directly, for training these people? Should that be a part of the TSA responsibility to do that? How do we get an assurance that these people are receiving sufficient training?

Mr. WYTKIND. Thank you for that question. I think we separate freight from Amtrak in a couple of ways but, overall I think you need strong training mandates the way this Committee has provided mandates in the airline side and then you need strong oversight to make sure the Department of Homeland Security actually carries out its mandates. Because that's part of the problem. This Committee mandated flight attendant security training after 9/11 and to this day TSA has not provided the kind of guidance that you asked for in this Committee or actually directed the TSA to do so. But I think the issue for Amtrak is one of resources and the mandate on Amtrak, if it doesn't also correspond to some financing and support for security upgrades across the board, including training, we're afraid that it's not going to get down to the rank and file level.

On the freight side, these are very cash rich companies that spend enormous sums of money on operations, efficiencies, infrastructure and as we've heard this morning, obviously on some security or maybe a lot of security. What we would argue is that if you put the mandate in the law, like you have in the current bill pending for this Committee, then the railroads will be required to finally make sure that their rank and file workers are getting trained. I think it's that simple but it requires a strong mandate out of this Committee and then it requires strong oversight of the DHS to make sure they actually carry out their regulatory responsibilities. Thank you.

The CHAIRMAN. Thank you, Senator. Senator Rockefeller?

STATEMENT OF HON. JOHN D. ROCKEFELLER IV, U.S. SENATOR FROM WEST VIRGINIA

Senator ROCKEFELLER. Thank you, Mr. Chairman. I'm giving myself double coverage in hopes that I might be heard. Let me ask Mr. Hamberger, it hasn't been gone into deeply here but, I think you made in your statement something which maybe harbingers what you may be going for later on and that is to have the Federal Government deciding what chemicals are safe to carry and which ones aren't. Now, a number of years ago, I guess it was after the *Exxon Valdez* thing, all ships had to double hull. You have some presumably in stock that are double-hulled. Explain to me why all of your stock is not double-hulled, even under the circumstances in which the chemical companies, which I am very, very sorry, are not represented here today because that precludes us from having a good discussion. I don't know why they weren't invited but, I regret that. Why is it that you just can't double hull or whatever is the corresponding guarantee of safety that the shipping industry went through.

Mr. HAMBERGER. I appreciate that question Senator because it is a very important issue. In fact, I was a little late for the hearing this morning because we had a conference call with members of the American Chemistry Council (ACC) to discuss the fact that in my testimony, there is a sentence that says long-term, it should be a policy to look for safer chemicals. It is a little bit of a different issue from the double hull because this is really more of a security issue than a safety issue. We can require tank cars to double hull, we can do everything possible but, there is no way long term to ensure against a terrorist attack. The only way to ensure that a community through which hazardous material is moving is safer, would be to have that hazardous material be less toxic.

Senator ROCKEFELLER. Do you routinely use GPS and other systems to always——

Mr. HAMBERGER. About 45 percent of the locomotives do have GPS. We're moving to 100 percent.

Senator ROCKEFELLER. On all of those that carry chemicals that are potentially in danger, are they covered by the GPS?

Mr. HAMBERGER. I don't have the answer to that.

Senator ROCKEFELLER. Isn't that fairly important?

Mr. HAMBERGER. I just don't know the answer.

Senator ROCKEFELLER. Yes.

Mr. HAMBERGER. But we do have the immediate capability of locating all locomotives.

Senator ROCKEFELLER. You all make a lot of money and I know that you always declare yourselves revenue inadequate, we won't get into that today.

Mr. HAMBERGER. Thank you.

Senator ROCKEFELLER. But, I look forward to having your annual reports. But, the chemical companies are merging and having all kinds of problems. Now, not to the extent that the airlines are. Railroads are an absolute necessity for this country.

Mr. HAMBERGER. Yes, sir.

Senator ROCKEFELLER. This country could not exist without them. So, two questions. One, why doesn't industry just go ahead and double hull or whatever the proper word is, as a matter of course? Because nothing has changed since 9/11 fundamentally. Part of that is the Federal Government's report, I mean, the report we were meant to have gotten and still hasn't arrived, which doesn't speak very well for us but, why can't you go ahead and do something which doesn't, you know, somebody puts a bomb underneath the track, double-hull isn't going to do it or whatever the comparable thing is. But, there are ways of racheting up.

Mr. HAMBERGER. Yes, sir.

Senator ROCKEFELLER. Safety which can help——

Mr. HAMBERGER. And in fact we are working very closely with the tank car manufacturers and ACC in determining whether or not there is a safer design. We are taking a close look at that and we're not going to mandate that but——

Senator ROCKEFELLER. What does that mean? I mean, you know that if you have two layers of hard metal around something it's going to be safe, so what does it——

Mr. HAMBERGER. Well, frankly Senator, that has cost implications for our customers, the chemical companies. The fact that we have moved 99.998 percent of the hazardous materials without accidental release calls into question whether or not that meets the cost-benefit test. There are about 12,000 tank cars out there. It would cost $1.2 billion to replace the fleet and so you want to make sure that the cost-benefit analysis is observed.

Senator ROCKEFELLER. Is the cost-benefit analysis which ultimately resolves what the railroad car safety matter will look like?

Mr. HAMBERGER. Obviously, if we were to make the skin of the car 2–3–4 inches thick, it would be much safer. But then the payload would be much less. So, there is that balance. And it is the chemical companies, as you know, who own the cars. We have to work with them in determining what is the appropriate standard.

Senator ROCKEFELLER. Well again, $1.2 billion is a lot of money. On the other hand, if you have an explosion because you have 99.998 percent—in the Intelligence business, that doesn't impress anybody because it's always the .2 percent.

Mr. HAMBERGER. Yes, sir.

Senator ROCKEFELLER. Which is going to happen. So, you're betting the farm on something not happening because it hasn't. Well, I mean, we've got reams of studies about 9/11 which proved that was not a very forward-looking aspect in terms of national security and what could we have done and people have come up with all kinds of answers. But, I really think that it's going to cost us money and therefore we shouldn't do it, even though you agree that it would make it safer is a little difficult for me.

Mr. HAMBERGER. I appreciate that input Senator. I will take that back to the tank car committee and when we get push-back from the chemical companies and tank car manufacturers, I'll invoke this conversation.

Senator ROCKEFELLER. Can I go to that tank car committee meeting too?

Mr. HAMBERGER. We'd love to have you.

Senator ROCKEFELLER. OK, now Mr. Wytkind?

Mr. WYTKIND. Yes?

Senator ROCKEFELLER. Do you think——

The CHAIRMAN. Could we move along a little bit?

Senator ROCKEFELLER. I'll stop.

The CHAIRMAN. We have each taken 5 minutes.

Senator ROCKEFELLER. Well then, I'll stop.

The CHAIRMAN. Do you want to ask your question?

Senator ROCKEFELLER. No, not if it breaks the 5-minute rule.

The CHAIRMAN. Senator Nelson?

STATEMENT OF HON. E. BENJAMIN NELSON, U.S. SENATOR FROM NEBRASKA

Senator BEN NELSON. Thank you, Mr. Chairman. Mr. Hamberger, I understand that before I arrived this morning that you made reference to the importance of getting TRIA, Terrorism Risk Insurance Act reenacted this year, re-authorized or put in place for the future. I share that view and I hope that we will be able to get the support that we need to get that in place.

Mr. HAMBERGER. Thank you, Senator.

Senator BEN NELSON. In the Committee's bill, it focuses on threats about high hazard materials and a lot of the discussion this morning has already been about that and there have been a number of recent accidents, as we know, South Carolina and Texarkana. It all reminds us of the dangers that an accident that involves toxic chemicals can really present to the public at large. Particularly those that are somewhere in the proximity of rail traffic. If you were required as S. 1052 contemplates to develop threat mitigation plans for high hazard hazardous materials traveling in specific rail quarters in a high threat area such as Washington, D.C., can you tell me why the DHS shouldn't have some authority, some relationship with the question of the security aspects of it, if not the safety, but at least with respect to the security aspects?

Mr. HAMBERGER. Before Senator Rockefeller leaves, I would like to say that it is indeed a bet-the-farm issue for us when we move this material. As I pointed out in my testimony, given the limitations on insurance and given that our common carrier obligation, requires us to move hazmat, it clearly is a bet-the-farm situation for our railroads. In fact, Senator, we are working with TSA and the Department of Homeland Security in developing risk-assessments for high hazardous materials corridors. Four, I believe, have been completed for Washington, New Orleans, Cleveland and New Jersey. We will continue to work with them to identify the risks and then put in place countermeasures for those corridors where high hazardous material does move.

Senator BEN NELSON. Well, I have talked to some of your members and I know that there is a significant interest on their part to make the rail traffic safer and more secure.

Mr. HAMBERGER. Yes, sir. And I think one of the questions is, once, if a plan is adopted and reduced to a regulation or has to go through a governmental approval process to change, then we believe we will not be as nimble as we need to be. For example, using Rita and Katrina as examples, our members acted immediately to detour materials out of the hurricane area up through Memphis and Kansas City. We want to work with the agency to develop the plan, but not have it as a mandate or regulation that would require an approval process before we can implement change based on intelligence we might get from the National Joint Terrorism Task Force, for example.

Senator BEN NELSON. Now, the rail industry hauls various pieces of equipment on the track, some of which may belong to the rail industry but, some of which may not belong to the rail industry. Who owns the tank cars that Senator Rockefeller was asking about, for example?

Mr. HAMBERGER. The tank cars are owned by the chemical companies or by a leasing company that leases them to the chemical companies. We do not own them.

Senator BEN NELSON. So they are, as opposed to let's say box cars?

Mr. HAMBERGER. That is correct. We own a substantial amount of the box car traffic or the gondola traffic cars but, none of the tank cars.

Senator BEN NELSON. Mr. Crosbie, in conjunction with the cost of security and who pays for the cost of security, obviously, with respect to air traffic, there's an addition to the ticket, $2.50 per segment for air travel. What kind of a push back could you possibly get by adding that kind of a surcharge, if you will, or security charge as more properly described, what kind of a push back could you possibly get for adding some of the cost of security for travelers?

Mr. CROSBIE. We have one that occurred, I'd say that it happened before my time with Amtrak, I joined Amtrak in 2003, January of 2003 and at the time, as I understand it, there was a push back from the states on basically, increasing the fares and you've seen, I think, some of that recently as well on the Northeast Corridor related to fares or reductions on discounts are sensitive——

Senator BEN NELSON. Nobody likes the security charge on the airline tickets, we've had discussions here about the fact that if you travel non-stop from Washington to L.A. you paid one surcharge and one security charge, if you go where it said to stop in between, you have to pay for both segments which could be the $5 dollars versus the $2.50 that you pay if you fly non-stop on a longer journey. I mean there are all kinds of questions about it but, it does seem reasonable to expect that the travelers would pay part of that security charge.

Mr. CROSBIE. We've certainly considered it.

Senator BEN NELSON. You certainly didn't have a lot of competition to worry about in terms of passenger rail travel.

Mr. CROSBIE. And we can go back and revisit it again. We certainly haven't ruled it out, we never have ruled it out. But, like I said when we proposed it in the past, it was not received well throughout the Northeast Corridor.

Senator BEN NELSON. I would imagine. I didn't receive it very well when they added it to airline travel. But, it's always a question of not only how much, but who pays? So, I appreciate the fact that you will take another look at that. Thank you, Mr. Chairman. My time is up.

The CHAIRMAN. Thank you, I appreciate that line of questioning, I've sort of been playing the bad guy here, before you got here, Ben. But I do think there has to be some examination of this, because there is a limit to how much more we can allocate for Federal funds and I think Amtrak is vulnerable now, because of the failure to find some way to increase revenues, I really do. Mr. Hamberger, I hate to tell you, but after the big Valdez disaster, I was the one that went to London.

Mr. HAMBERGER. Yes, sir.

The CHAIRMAN. And came back and said that the only answer was to double-hull those tankers and people didn't like me at all. You better listen to these guys. Someone ought to test whether double-hulls on these tank cars will provide additional security because I think right now the attitude in Congress would be to mandate that all of those cars carrying chemicals be double-sided. And the only thing that is going to deter that would be sufficient proof that it wouldn't make any difference. If that won't make a difference then I would urge you to go and look and see what we're doing in Iraq by some of the changes that are classified as a matter of fact to the tank cars that are carrying fuel or the trucks that are carrying ammunition. They have new facilities, new ways to improve the safety for those people driving those by virtue of changes that have been made in country to those tanks and those trucks.

And, I think Congress right now would be in the mood to say that is a risk that should not be, that the cities of the country should not be exposed to that risk if it really exists.

Mr. HAMBERGER. In fact Senator, we are working on a polymer additive at our Pueblo rail research facility, the Transportation Technology Center. It was developed for the Iraq environment to see whether it can make the tank cars more impervious. It is also a self-sealant so that if there is a breach, it would self-seal. So, you are absolutely right and I appreciate that.

The CHAIRMAN. Thank you very much, thank you all very much for coming. I appreciate it and we will continue to consider this bill that Senator Inouye and I and others have introduced.

[Whereupon, at 11:37 a.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF HON. MARK PRYOR, U.S. SENATOR FROM ARKANSAS

I would like to thank Chairman Stevens and Co-Chairman Inouye for holding this hearing on rail security this morning. It is a very timely hearing Mr. Chairman, especially for Arkansas. As many of you have read, just last Saturday we had a tragic accident in Texarkana, Arkansas. A Union Pacific train coming into station collided with another Union Pacific train that was stationary on the tracks in the Texarkana rail yard. The resulting explosion killed one Arkansan, hospitalized 20 others, destroyed two homes and a rail bridge, and temporarily evacuated close to 700 people from their homes.

The gas that caused the explosion, propylene, is a respiratory toxicant that is abundantly produced in this country, typically used in the production of plastics and rubber. I am sorry that this accident happened, and I don't know the cause. I do know that the Federal Railroad Administration and the National Transportation Safety Board are already investigating, and I hope they have a report that will tell us the cause of this terrible accident soon. I also hope that they will keep me informed of the progress of the investigation as it moves forward.

I have a couple of observations I would like to make in regards to this accident. First, my thoughts and prayers are with the family of the individual who was killed as well as the families whose homes were destroyed or damaged as a result of the accident. Second, I would like to publicly recognize the first responders of Texarkana who responded so quickly to the explosions and kept fires from spreading to many, many other homes in the area. This could have been a much larger disaster but for their efforts.

Mr. Chairman, it is time that we ensure governments—local, State, and Federal have the plans in place and the resources in place to be able to quickly respond to accidents or terrorist attacks throughout our rail system. It is too important. Too many people and too many essential commodities move through the system each day to ignore the risks inherent in the system. The first thing we must do in order to put these plans in place is to conduct a risk assessment. You can't decide where to spend precious resources unless you know where the threats are. I encourage the Transportation Security Administration and the Department of Homeland Security to work in coordination with the Federal Railroad Administration and Department of Transportation in conducting this risk assessment as quickly as possible. After performing the assessment, we must move forward to ensure that workers are properly trained to recognize safety risks and threats, and we must ensure that appropriate technologies are developed and utilized to protect our vital rail infrastructure.

I look forward to discussing rail security with all the interested parties, including industry and labor as well as the Administration and my colleagues in the Congress. I am happy to be a cosponsor of S. 1052. the Transportation Security improvement Act of 2005, and look forward to the thoughts of the witnesses on the rail aspects of this important legislation. I thank the Chairman and Co-Chairman.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO CATHLEEN A. BERRICK

Question 1. The rail provisions of S. 1052 include security upgrades, threat assessments, security training, research and development, and several other important initiatives, many of which were unanimously approved by the Senate last year. What is your position on the rail provisions of S. 1052? How can we improve them?

Answer. Our comments on the rail provisions of S. 1052 pertain to those affecting passenger rail operations. In general, we concur with the provisions recommending that grants be awarded to upgrade rail security. Some of the upgrades identified in the proposed legislation, such as implementing public secure awareness campaigns for passenger train operations, employee security awareness programs, and emergency response training, reflect practices we have observed in our recent work on rail security. It will be particularly important, as noted in the legislation, for improvements in these areas and others to reflect the results of vulnerability and risk assessments conducted by the Transportation Security Administration (TSA), the Department of Transportation (DOT) and other appropriate agencies that identify critical rail assets.

On the issue of rail risk assessments, we support the creation of a task force to ensure that these assessments are completed and critical assets and infrastructure and related vulnerabilities are identified. It is unclear, however, if the task force is meant to include non-federal stakeholders such as rail industry associations and regional passenger rail agencies. We encourage the inclusion of these non-federal stakeholders in the risk assessment process to leverage their expertise. Consistent with Homeland Security Presidential Directive 7, we believe that it is important that these assessments incorporate an overall methodology that will enable different rail assets to be evaluated on a consistent basis. We also recommend that funds disbursed to Amtrak for system wide security upgrades be based on a comprehensive terrorism risk assessment and response plan that provides a baseline for investment prioritization and decision making. During our review of passenger rail security, we observed that Amtrak had not yet completed such a system wide assessment.

With regard to the provision (Sec. 314(b)) instructing TSA to review existing DOT regulations to identify areas where regulations need to be revised to improve security, we believe that other actions may also be taken to strengthen security. Specifically, we believe that TSA should review existing rail security regulations, directives, and standards and report to the Committee the results of its review of (a) an assessment of whether established security regulations, directives, and standards are consistent with industry best practices, and (b) a plan and schedule for rail inspections to be conducted by rail security inspectors. We further recommend, based on unique security practices observed in foreign countries during our review, that the Department of Homeland Security evaluate the feasibility of establishing and maintaining an information clearinghouse on existing and emergency security technologies and security best practices used in the passenger rail industry both in the U.S. and abroad. We further recommend that the Department be required to evaluate the potential benefits and applicability of implementing covert testing procedures to evaluate the effectiveness of rail system security personnel, practices used by foreign rail operators that integrate security into infrastructure design, and random searches and screening of passengers and their baggage, pending the results of and ongoing joint Federal and industry review of the impact of random screening on passenger rail operators.

Question 2. During GAO's investigation on passenger rail security, did you have an opportunity to review a preliminary version of the National Strategy for Transportation Security? Now that it has been released, do you think it addresses some of the concerns that you identified in your report, particularly your concerns regarding the lack of a coordinated plan for rail security?

Answer. We did not have an opportunity to review a draft of the NSTS during our recent audit work on rail security because, according to TSA, the document was not available before we completed our work. We believe that the NSTS since issued by DHS provides a broad framework for conducting transportation risk assessments, and is a first step for determining how critical transportation assets are to be evaluated for protection. However, we believe that the strategy as written is too general to address our concerns about how risk assessments are actually to be conducted and how stakeholders are to be involved in the process. It is also not clear from the strategy how assets within different transportation sectors, such as passenger rail and aviation, are to be compared in order to prioritize risks and allocate resources. Nor does the strategy include transportation modal security plans, as required by the Intelligence Reform and Terrorism Prevention Act of 2004, although broad elements of modal strategic plans are discussed. Other strategic planning documents that TSA is expected to issue in 2006, such as the Transportation Sector Specific Plan, may include these specific details not contained in the NSTS. We believe it is important that more specific information related to the Department's strategy for securing all modes of transportation be developed, coordinated, and shared with appropriate stakeholders, beyond what is published in the NSTS.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO EDWARD R. HAMBERGER

Question 1. As the representatives of the major sectors of the railroad industry, you live with the challenges of securing your railroads everyday. We have tried to craft a bill that will help make this job easier. Yet, I'm sure we can do more. Can you tell us which of our provisions you feel are most needed and why? If there were one thing more we could do in this bill to help you reach your goal of a safe and secure railroad and workplace, what would it be?

Answer. The AAR supports provisions in the bill that call on the Administration to develop a comprehensive security plan that includes the identification of the most important rail assets and the identification of the biggest threats to those assets. In developing this plan, the government should use the AAR's Security Plan as its basis. Additionally, freight railroads should be able to apply directly for rail security grants rather than have to go through the states. The AAR also fully support funding for research and the deployment of rail security technologies, including automated security inspections, infrastructure integrity monitoring systems, emergency bridge repair and replacement, communications-based train control systems and tank car vulnerability reductions.

One additional measure that the bill could address concerns the use of the National Guard and local law enforcement support to augment industry protection of critical infrastructure. To date, railroads have been underwriting the cost of security measures for the general public and national defense. Protective measures that would be required at the highest alert levels could not be sustained by the rail industry alone. Rail security legislation could make clear that states would be reimbursed by the Federal Government for costs associated with increased protection of critical rail infrastructure assets under heightened alert conditions.

Question 2. The Committee's bill, S. 1052, focuses on the threats posed by the rail shipment of "high-hazard materials" and requires railroads to develop threat mitigation plans. While the safety statistics you quote are impressive, recent accidents in Graniteville, SC and Texarkana, AK, remind us of the dangers that an accident involving toxic inhalants and explosives presents. If you were required, as S. 1052 contemplates, to develop threat mitigation plans for high-hazard hazardous materials traveling in specific rail corridors in high threat areas, such as Washington D.C., why should the DHS not have the power to approve those plans? If there is no approval or enforcement authority, how can anyone be sure that the plans are adequate?

Answer. The AAR and member railroads are working with TSA and the Department of Homeland Security in developing risk assessments for high hazardous materials corridors. Four have been completed to date including Washington, New Orleans, Cleveland and New Jersey. We are continuing to work with these agencies to identify risks and put in place countermeasures for those corridors where high hazardous material moves. We have consulted and conferred and they have not taken exceptions to our plans. Further, on request, railroads have altered their operations and cooperated with DHS for special situations and events.

The USDOT, both under the Federal Rail Safety Act and the Hazardous Materials Transportation Act, already extensively regulates the safe transportation of hazardous materials. The Research and Special Programs Administration (now the Pipeline and Hazardous Materials Safety Administration, PHMSA) regulation HM–232, published in 2003, requires railroads to develop and implement security plans when transporting hazmat. This agency also has oversight authority for the implementation of these plans.

If legislation requires a governmental approval process for threat mitigation plans, we believe that it could actually jeopardize security by limiting the ability of the railroads to respond to quickly changing circumstances. The response of the railroads after Katrina and Rita is illustrative. The railroads were able to act immediately to detour hazmat materials out of the hurricane area using a routing plan specific to that particular situation and without having to wait for an approval from Washington.

To implement this provision as written, DHS would have to develop criteria to define a satisfactory threat mitigation plan. Such criteria would no doubt be promulgated by regulations. Regulations, then create a certainty as to what the railroads are or are not doing, when for true security, uncertainty is best. Equally, situations could occur where railroads would need to alter their plans on short notice but could be hamstrung by conflicting regulatory requirements. DHS already has the authority to review our transportation security plans. We believe that the most effective approach is to work in consultation with DHS rather than a Federally-directed command and control effort.

Question 3. In your written statement you also oppose the provision in our bill, Section 310, which requires that DHS and DOT in consultation develop and issue guidance on rail worker security-training programs and to review and approve training programs submitted by railroad carriers. Do you believe the existing freight railroads security-training program is sufficient?

Answer. The AAR does not oppose the provision that would require DHS and DOT to develop and issue guidance on rail worker security training or to review the security training programs advanced by railroad carriers. The AAR opposes the institution of a Federal approval process for the railroads' security training programs for the following reasons. First, a Federal approval process tends to make it difficult for the industry to adapt quickly to new circumstances and adjust security training requirements on a real time basis. We are concerned that railroad workers would then refuse to undertake any security training unless it was specifically approved by the Federal Government. Second, the provision unfairly singles out the railroad industry—as opposed to all manufacturing and service industries—as requiring Federal approval for corporate training practices.

Since the days of railroad bandits and terrorist outlaws, the Class 1 freight railroads have employed and maintained their own railroad police forces to help protect the security of its employees, passengers and freight. Some 2000 railroad police are employed today as duly appointed sworn law enforcement officers certified or commissioned under State and Federal statues. Reacting swiftly to the events of September 11th, the major railroads put into place more than 50 countermeasures to ensure the security of the industry. Access to important rail facilities and information was restricted. The industry significantly increased cyber-security procedures and techniques. Employee records were compared with FBI terrorist lists. Security briefings, like safety briefings, became a daily part of an employee's job. Some railroads have gone so far as to include security training as part of the annual FRA-mandated employee certification process. In an effort to further increase the level of security awareness for their employees, AAR member railroads are working with the National Transit Institute (NTI) at Rutgers University to develop a uniform security awareness curriculum that will significantly enhance the level of employee security training. The curriculum is modeled after the program NTI and the Federal Transit Administration developed for public transit agency employees.

The goal of the training is to provide rail employees with an understanding of their role and responsibility in system security and how to implement their companies' procedures upon detection of suspicious objects or activities. Course modules include instructions on reacting to threats, identifying suspicious activity, identifying suspicious objects, and responding to incidents. These course modules will be rolled out by the AAR member railroads within the next 90 days.

Question 4. How do you explain the disparity between AAR's perception of the rail workers' confidence in the security training they have received and the results of a recent Teamsters Union Rail Division survey in which 85 percent of those responding claim to not have received security training in the last twelve months?

Answer. Despite an enviable record of safety over more than two decades, some rail labor union leaders are attempting to attack the industry by tallying responses to a loaded union questionnaire and touting it as a nationwide "study" of security gaps on U.S. railroads. Union leaders more than a year ago gave the short questionnaire to members of the Brotherhood of Locomotive Engineers and Trainmen (BLET) and the Brotherhood of Maintenance of Way Employes Division (BMWED), both part of the International Brotherhood of Teamsters Rail Labor Bargaining Coalition. It carried a Teamsters logo and instructed members to "please give this form to your local chairman."

Teamsters admit their report is not a scientific analysis. In reality, it is a tactic aimed at the bargaining table that ignores the facts and misrepresents the industry's strong safety record.

The fact is that after 9/11, America's railroads worked quickly with Federal security agencies to develop and implement a multi-layered, risk-based security plan for the Nation's freight rail network that included security awareness training for rail employees. Since 9/11, freight railroads have implemented more than 100 new security actions and 50-plus changes in their operations. That's in addition to the intensive safety training required of all railroad operating employees and the special security training that all rail employees who handle hazardous materials movements receive.

The industry is currently working with the National Transit Institute (NTI) at Rutgers University to create an enhanced security awareness training program for railroad employees throughout the country.

America's freight railroads have developed train control technology that will improve significantly the safety of freight operations. This 21st Century technology will help to prevent train collisions, improve productivity and reduce accidents caused by fatigue and human error, the most common causes of train accidents. Taking the Nation's freight rail network to this next level of safety and success will require 21st Century labor agreements and changes to antiquated work rules negotiated years prior to these technological advances. U.S. freight railroads are now in negotiations with unions representing engineers and train crews—hence the interest of the Teamsters in discrediting the safety and security record.

Question 5. I would like to compliment the railroad industry for its commitment to Operation Respond. According to our information the Operation Respond software is now available to over 56,000 response agencies. Have the railroads given any thought to how this valuable connection with emergency responders can help them deal with communities concerns over railroad security? I am referring specifically to advanced information and rerouting of hazardous materials.

Answer. The Class 1 railroads have joined the Department of Homeland Security and the Department of Transportation in sponsoring Operation Respond, a public-private partnership that develops software, mapping systems, alert networks and training programs for community responders. The AAR supports Operation Respond financially and is a member of its Steering Committee. The AAR and Operation Respond signed an agreement in November 2003 to assist emergency responders, promote safety and increase security along our Nation's railroad system. This agreement includes the development of an "information sharing system" to benefit emergency responders and railroad carriers, and the integration of the Emergency Services Information Network Corporation (ESINC) network and the AAR Rail Alert Network.

The freight railroads work aggressively to make sure that railroad employees, first responders, emergency personnel and other necessary officials are prepared to respond quickly and efficiently. Railroads provide local emergency officials with information on the types of hazardous materials being transported through their communities. The railroads also work closely with Local Emergency Planning Committees to make sure they have comprehensive and up-to-date emergency planning information.

The Nation's freight railroads, both individually and in partnership with the American Chemistry Council (ACC), train more than 20,000 emergency responders each year in communities across the Nation. Railroad companies are active participants in the ACC's TRANSCAER® (Transportation and Community Awareness and Emergency Response), a nationwide effort to assist communities with emergency response plans as well as CHEMTREC® (Chemical Transportation Emergency Center), the ACC's 24-hour emergency response operation. TRANSCAER requires its industry partners to adhere to a rigorous code of management practices and strict standards for self-evaluation, systems management and performance measurement and mutual assistance. Under TRANSCAER, railroads bring hands-on and classroom training to thousands of emergency first responders. They also help emergency planning groups identify the general types of hazardous materials moving through the community; provide guidance for local officials to develop and evaluate their emergency response plans; assist with testing and training.

Railroads also participate in CHEMTREC, a 24/7 operation that provides immediate emergency response information and assistance during emergencies involving chemicals. Each CHEMTREC member puts CHEMTREC's number on its packages and tank cars. CHEMTREC maintains an extensive database of information on chemicals, shippers and emergency response, used by first responders during hazmat accidents. The railroads provide needed information to CHEMTREC during railroad accidents so that the information can be communicated to local emergency responders to help mitigate accidents.

Individually, railroads sponsor annual training for first responders across the country at the Emergency Response Training Center in Pueblo, Co. The training includes hazardous materials technician; tank car specialist; advanced tank car specialist; intermodal specialist; incident commander; advanced hazmat technician; highway emergency response; weapons of mass destruction; hazmat monitoring; and transportation specialist. The railroad industry sponsors an Annual Hazardous Materials Seminar attended by hundreds of emergency responders, shippers, contractors as well as railroad emergency response personnel to provide up-to-date training on the latest emergency response techniques and regulations. It also provides hands-on training to familiarize responders with equipment used in hazmat accidents.

In big cities, small towns, and rural areas, railroads work with communities to conduct full-scale emergency response drills that can take up to six months to plan and involve responders from local, county, state, regional and Federal levels. The railroads help planners include every public agency that needs to be notified and involves them in the drill. Drills are sometimes conducted across multiple towns and regions to test how well communities work together in an emergency situation.

Since 9/11, emergency training has also included a terrorism component. AAR member railroads own four tank cars that are used for both the emergency response drills as well as training purposes. Other safety initiatives conducted by various railroads include mock safety drills and table top simulations in communities; on-going assessments of potential risks to employees and local communities resulting from accidents or other emergencies; on-going training programs for those employees who have response or communications responsibilities in the event of an emergency; emergency exercises, at least annually, to test operability of written emergency response plans; facility tours for emergency responders to promote emergency preparedness and provide up-to-date knowledge of facility operations; special environmental monitoring teams, located along the railroad system, which can be immediately mobilized to relay information to health experts. These teams are equipped with advanced detection and monitoring equipment; audits of hazmat contractors to ensure that equipment, training and response capabilities meet standards; audits of internal operations and chemical shippers for correct shipping documentation; reviews of non-accident releases from tank cars and, if necessary, offers to retrain chemical shippers regarding safe loading and sealing procedures.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO EDWARD R. HAMBERGER

Question 1. Are all AAR member railroads offering security training for their employees?

Answer. All railroad employees have received security awareness training. Security is also a part of employees' daily job safety briefing. As a general rule we want our non-security employees to report suspicious activity to the railroad police so they can take appropriate action. We do not want non-security employees to put themselves at risk in addressing a security concern. Railroad employees will be briefed at daily job briefings when they need to take additional action and what that action entails.

Question 2. Do you believe that the Federal Government has a role in the development of uniform standards for employee security training programs?

Answer. The most effective role that the Federal Government can play with respect to employee security training programs is to share best practices information with the industry. The AAR is currently developing a uniform security awareness curriculum with the National Transit Institute that will be deployed throughout the industry in 2006 that significantly enhances the level of employee security training. The goal of the training is to provide rail employees with an understanding of their role and responsibilities in system security, and how to implement their companies' procedures upon detection of suspicious objects or activities. Course modules include instructions on reacting to threats, identifying suspicious activity, identifying suspicious objects and responding to incidents.

The Department of Transportation implemented security training requirements in 49 CFR § 172.704. Since the railroads already comply with the current regulations, and we have a system in place to instruct employees on what they will need to do at increased alert levels, we see no reason for additional regulations or standards.

The AAR does not believe it to be an appropriate Federal Government role to mandate uniform standards to the private sector for employee security training. Private industry inherently has an interest in the protection of its employees and assets and is in the best position to appropriately discern how best to train its workforce. Worker security training practices across manufacturing and service industries will vary greatly depending on many circumstances. What may be appropriate security training for a locomotive engineer will not be the same as for a hospital nurse, a cafeteria worker or a nuclear plant operator.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO WILLIAM L. CROSBIE

Question 1. As the representatives of the major sectors of the railroad industry, you live with the challenges of securing your railroads everyday. We have tried to craft a bill that will help make this job easier. Yet, I'm sure we can do more. Can you tell us which of our provisions you feel are most needed and why? If there were one thing more we could do in this bill to help you reach your goal of a safe and secure railroad and workplace, what would it be?

Answer. The Rail Security Act of 2005 provides the most comprehensive approach to improving rail surface transportation systems to date. Because of Amtrak's continuing fiscal uncertainty on future funding levels for the Corporation as a whole, the most needed provisions of S. 1052 for Amtrak are the rail security and life safety sections (Sections 303, 304 and 305). While Amtrak is currently committing capital resources to security improvements. it is critical that the Federal Government provide an equitable share of funding for the rail transportation mode.

Since 9/11, rail security issues and funding have been given short shrift. The most important thing that this Committee could do to help Amtrak reach its goal of a safe and secure railroad and workplace is, simply, to have this legislation passed and enacted.

Question 2. Amtrak has been very proactive in working with DHS/TSA and DOT/FRA to engage in pilot programs and other security activities. What additional assistance do you need, in addition to more funding, from the Federal Government to ensure adequate security for your passengers?

Answer. Amtrak believes that some of the initiatives it has coordinated with DHS/TSA provide a guide for government/industry relations that can reasonably improve rail security. An example is the use of TSA baggage screening personnel and equipment based upon certain events (RNC, Inaugural events). This ought to be extended to intelligence driven threats at specific locations or areas. In addition, systematic security schemes ought to be deployed and developed by government to keep terrorists off balance or to eliminate security predictability. Such efforts performed in coordination with rail agencies would improve rail security.

Intelligence information and sharing is one of the key elements for helping to secure Amtrak. Like all rail agencies, Amtrak needs to receive timely information to address threats. DHS/TSA must ensure that dissemination of threat information is performed in a quick and effective manner.

Because of the expanse of the Amtrak route system, Federal agencies ought to provide assistance to Amtrak upon request to support security initiatives (such as the TSA canine program). Consideration ought to be given to state and local agencies receiving grant funding for initiatives designed to improve rail and transit security.

DHS passenger rail and transit security grant programs should be expanded and used as models for development of integrated rail security plans and policies.

As stated in GAO report, 05–851, there needs to be a security technology clearinghouse established by the government that rail agencies can use to develop, coordinate or seek assistance in purchasing, implementing and improving equipment to protect rail security assets.

Question 3. Amtrak has shown leadership in its support of Operation Respond hazardous materials tracking technology, particularly as it relates to providing police and fire departments with valuable response guidance. If and when something does happen, the Operation Respond software is a valuable response tool for Amtrak. What do you think can be done to encourage a more widespread incorporation of the Operation Respond software by the communities Amtrak serves and the commuter rail industry?

Answer. First responder training grants have been available to state and local agencies for years. The grants are usually conditioned upon a Federal agency approving the course or actually providing the course. A possible method of expanding the use of the Operation Respond program would be to allow first responders to receive funding for Operation Respond training, to have Federal agencies conduct and/or approve training and funding for Operation Respond training, and/or to condition grant funding for first responders to take also Operation Respond training. An evaluation of the ability of Operation Respond to handle increased training demands should also be explored and/or funded.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO EDMUND "KIP" HAWLEY

Question 1. I have worked hard, together with Chairman Stevens, to craft a solid blueprint for future Federal actions to secure our Nations' railroads. The rail provisions of S. 1052 include security upgrades, threat assessments, security training, research and development, and several other important initiatives, many of which were unanimously approved by the Senate last year. Yet, if we can strengthen our efforts, we must. I hope each of you will help us do that. What is your position on the rail provisions of S. 1052? How can we improve them?

Answer. The Department's views on S. 1052 were sent to the Committee on November 10, 2005. We stand ready to render any technical assistance that the Committee may request.

Question 2. In less than a year and a half, terrorists have killed almost 300 people in bombings of mass transit systems, most recently in London and in Madrid. Yet, this summer, Secretary Chertoff indicated in an interview that the protection of transit and rail should largely be the responsibility of cities and states and not the Federal Government. Do you believe that funding for rail and transit security is a lower priority for the Federal Government than for other transportation modes?

Answer. The Transportation Security Administration (TSA) and the Congress have focused the majority of transportation security funding towards what has been considered the largest and most consistent potential threat—attacks on our aviation system. At the same time, TSA has been working to improve security in other modes of transportation. The Nation's transportation system is vast and complex, but historically only in aviation security is the Federal role direct and pre-eminent. For that reason, TSA and the Department of Homeland Security (DHS) have known that the aviation model of security would not work for securing other modes of transportation. Thus, the Department, in coordination with TSA continues to work with State, tribal, local, regional and private partners to help secure our transportation system. These efforts span the spectrum of security, from intelligence and information sharing to awareness through prevention, response, and recovery from a potential terrorist attack in the United States.

The responsibility for securing our Nation's transportation system is a shared one between Federal, State, and local governments, and private industry stakeholders, and system users. Public and private stakeholder investment in security is both appropriate and expected. Currently, the Federal Government is providing funding, in the form of security grants, to help ameliorate the cost borne by the private stakeholders. TSA and ODP will continue to assist system operators identify their security risks through: (1) security assessments, both government-facilitated and through use of self-assessment tools, (2) compliance efforts, and (3) through cooperative partnerships with industry associations and operators to develop effective and cost-efficient mitigation strategies.

An example of a cooperative partnership is the work that DHS, including TSA have done and continues to do with Amtrak. TSA has provided explosives detection canine teams to Amtrak upon its request on several occasions, including during the Republican National Convention, Inauguration and in New York during the fall 2005 security alert. TSA is engaged in a continuous dialogue with Amtrak regarding use of canine resources and is exploring the possibility of instituting a more formal framework for providing such support to Amtrak in the future. TSA fully integrates Amtrak into its security planning and is working to further enhance information and intelligence sharing capabilities.

Question 3. I am sure you are aware of the recent survey of the DHS staff that showed a low morale. You are new to the Agency, or rather, returning to it. How do you plan on addressing the morale issue?

Answer. Workforce morale is very important to me and I am pleased to say that the Transportation Security Administration (TSA) has taken a number of actions to improve morale since we initially surveyed our entire workforce in February/March 2004, which was followed by a resurvey of a sample of our workforce by the Office of Personnel Management (OPM) and the Department later in 2004. Our Corporate Organizational Action Plan outlines the broad interventions that fall under four general areas that were highlighted as important for change: fairness and treatment of others, rewards and recognition, communication, and work environment/quality of worklife. Additionally, our recently published TSA Compendium of Positive Practices identifies interventions that can and have been taken by local leaders to address workplace and workforce issues in a variety of areas.

Underlying the first two areas was a general sense that outstanding performance does not result in any tangible rewards, such as increased pay or bonuses, promotional opportunities or other career advancement. I am pleased that both national and local rewards and recognition programs have been established since the survey was administered. These programs allow for both monetary and non-monetary recognition for a job well done. A screener performance management system is being designed that will better identify top performers and link their outstanding performance to pay increases. This system will consider objective measures of performance, assessment of competencies and will incorporate continual feedback and coaching as critical components. We will continue to seek suggestions for ways to publicly recognize and reward those who do an outstanding job for TSA, both at the national as well as the local, airport level.

Expanding career opportunities for our screener workforce is very important to me. I recently announced a change in the job series and title for TSA screeners that better signifies the important professional role that they serve. We will also be establishing intern programs that will assist members of our workforce to transition into Federal Air Marshal and Inspector positions. I have decided to reserve some Federal Air Marshal openings to be filled exclusively by TSA employees. We currently have a variety of career planning services available to TSA employees, including a career coaching service to help guide employees in identifying career interests, conducting job searches, and developing effective application materials. We also have a web-based Career Toolbox to support employees' career planning.

Communication is also critical to employee morale. An important aspect of that is to give employees at all levels a voice in matters that directly affect them. To that end, there are initiatives at many airports across the country to do this, many of them folded under broader Model Workplace Programs—town hall meetings, screener advisory groups and small on-site meetings through which action plan results for an individual work location are fed back directly to the employees who work at that site. At the national level, we have the Employee Issues Coordination Council, bringing together organizations that deal with employee issues, to provide a corporate focus and clearinghouse for information on employee issues as well as to collect and analyze information on employee issues, recommending corporate priorities for action.

I have personally conducted numerous town hall meetings, both in Headquarters and in airports across the country, since rejoining TSA. Visible and empowering leadership is important. Role clarity is essential to achieving optimal action planning and results. We must highlight the leaders who are accountable and celebrate those who achieve results. At a national level, I've announced the establishment of a Screener Advisory Group and an Assistant Federal Security Director Advisory Group. As their first charge, I have asked both groups to propose a set of incentives that they believe are key to retaining our most talented employees, and I eagerly await their suggestions.

We are also taking steps to address concerns related to the quality of the work environment. Of utmost concern to me is the safety and well-being of our workforce, particularly the screener workforce. I will be focusing additional attention first on preventing injuries and second, getting employees back on the job as soon as possible. The physical work environment of many of our screeners continues to require the attention of both local and national leadership. I am pleased that many improvements have been put in place already and others are underway in airports across the country.

Finally, it is important to continually assess employee morale and whether the programs put in place make a difference. To that end, we expect to again survey the entire TSA workforce in early 2006 to see whether morale has improved, and in what areas. With those results, we will be able to determine where additional effort and/or resources must be focused to achieve further gains. Additionally, in November 2005, TSA launched a National Exit Survey for departing employees, with the same end in mind.

While I am pleased that some progress has been made, I recognize that we have much more work to do. It is a challenge that is worth the effort—to create the model workplace and become an employer of choice.

Question 4. How many staff does TSA have dedicated to rail security—people whose primary job functions is to work on rail security issues? How many people whose primary function is working on non-aviation security issues? How many staff working on aviation security issues?

Answer. The Transportation Security Administration (TSA) is basing its answers to these inquiries on an analysis of the funding source for the salaries and benefits of TSA employees.

As of October 15, TSA staff includes a total of 116 individuals dedicated to rail security, including 96 Rail Inspectors. The total number of individuals whose primary function is on non-aviation security issues is 220. This figure includes the 116 dedicated to rail security. Employees paid from the Aviation Security budget category, which include primarily security screeners, total about 51,440.

TSA notes that these totals do not include individuals serving in cross-cutting areas such as credentialing, intelligence, and administrative support.

Question 5. What percentage of TSA funding, apart from grants are directed exclusively to rail security? How much is that in comparison of funding directed exclusively to aviation?

Answer. Under the Homeland Security Appropriations Act, 2006 (Pub. L. 109–90), Congress appropriated funding to the Transportation Security Administration (TSA) as follows:

- $4,607,386,000 for necessary expenses relating to providing civil aviation security services;
- $36,000,000 for necessary expenses related to providing surface transportation security activities;

- $74,996,000 for necessary expenses for the development and implementation of screening programs of the Office of Transportation Vetting and Credentialing;
- $510,483,000 for necessary expenses relating to providing transportation security support and intelligence; and
- $686,200,000 for necessary expenses of the Federal Air Marshals Service.

Of the $36 million for surface transportation security activities, Congress directed that $8 million be set aside for the rail inspector program and canine teams. TSA also intends to spend approximately $8 million for rail security efforts in FY 2006, for a total of about $16 million.

However, this number is not reflective of all efforts directed towards rail security either within TSA, the Department of Homeland Security (DHS), or the Federal Government. First, it should be noted that other efforts and funding streams within TSA, particularly under the transportation security support and intelligence category, contribute to rail security efforts. For example, cross-cutting offices, such as the Chief Technology Office, Office of the Chief Counsel, Transportation Security Operations Center, Human Resources, Chief Information Officer, and Transportation Security Intelligence Service, provide support to all programs within TSA, including the rail security programs. Specifically, TSA and the Department have focused significant resources on intelligence with the goal of identifying and stopping a terrorist before he reaches the intended target. Because of these cross-cutting offices and other Departmental efforts, it is impossible to parse a percentage of funds spent exclusively on rail or aviation.

Additionally, Congress has funded programs for infrastructure protection and research and development through other DHS entities. TSA works closely and its programs align with the Information Analysis and Infrastructure Protection (IAIP) and Science and Technology (S&T) Directorates efforts on rail and infrastructure security along with the Department of Transportation's modal administrations efforts in rail. In summary, TSA's spending on rail security is obviously significantly less than the amount spent on aviation security. That is the result of the congressionally mandated security role TSA provides in aviation by screening passengers and baggage versus a more standard-setting and compliance role that it plays in rail security.

Question 6. TSA may use "risk/value analysis," but will the funding & staff be there to address the risks?

Answer. As indicated above, Congress recently appropriated funding for the Transportation Security Administration (TSA) for FY 2006, and TSA will manage the level of resources that have been made available by utilizing a threat-based, risk-management approach to transportation security. TSA constantly reassesses these resources and budget priorities as part of the Department of Homeland Security's (DHS) risk-based management approach to securing the Nation's critical infrastructure. In addition, since the creation of TSA, Congress has provided very specific direction as to how funds are to be spent. TSA is responsible for evaluating risk to the transportation system across a changing array of threats, sharing threat and risk information with transportation stakeholders (public and private), establishing consistent national transportation security standards across all modes, monitoring compliance with those standards by transportation stakeholders and in the event of a transportation security incident, ensuring rapid restoration of service and public confidence. TSA and our partners within DHS, in coordination with the Department of Transportation (DOT), have conducted vulnerability assessments on transportation assets, such as rail and transit, to determine their susceptibility to attack or compromise.

Ensuring that our Nation's transportation systems are secure must be accomplished through effective partnering between appropriate Federal, State, local and private industry entities. Of course, DHS is charged with the responsibility for protecting all modes of transportation, but it has consistently held that this responsibility must be shared with Federal, State, local and private industry partners, many of whom were already in the business of providing security for their particular piece of the transportation puzzle. The Administration and Congress have recognized the importance of supporting these efforts through grants to our governmental and industry partners. In the Homeland Security Appropriations Act, 2006 (Pub. L. 109–90), the Office for Domestic Preparedness will mange the following transportation security programs as directed by Congress to include the following:

- Rail and Transit Security—$150,000,000
- Port Security—$175,000,000
- Intercity Bus Security—$10,000,000
- Trucking Security—$5,000,000

Additionally, DHS has allocated $8.6 billion since its creation for counterterrorism preparedness. These funds can be allocated by State and local governments for rail security efforts.

Question 7. How much of the Transit Security Grant Program funding has been actually obligated? What percentage of this has gone to freight rail security?

Answer. In FY 2005, Congress directed that $150 million be made available for rail and transit security grants. Of these funds, the Department of Homeland Security's Office for Domestic Preparedness (ODP) made available nearly $134 million under the Transit Security Grant Program (TSGP). To date, ODP has obligated all funds under the TSGP. While none of these funds were awarded to promote freight rail security efforts, the Department did make available $5 million from the remaining rail and transit security grant funding provided by Congress for a Freight Rail Security Program. This $5 million was awarded to the Railroad Research Foundation to undertake three projects: (1) development of a Rail Corridor Risk Management Tool; (2) development of a Rail Corridor Hazmat Response and Recovery Tool; and (3) development and demonstration of "Safe Haven" concepts for in-route toxic inhalation hazard shipments. These projects were made available and are being managed by the Office for Domestic Preparedness as identified through partnerships with other DHS entities, including TSA, the Border and Transportation Security Directorate, and the Information Analysis and Infrastructure Protection Directorate, as well as with the Federal Railroad Administration and the Pipeline and Hazardous Materials Safety Administration within the Department of Transportation. These projects offer the potential for long-term enhancement of freight rail security.

Question 8. In June 2005, Mr. Ed Wytkind, President of the Transportation Trades Department, AFL–CIO, sent a letter to Secretary Chertoff outlining several concerns over the status of transportation security in this country. Specifically, the letter points out that no Federal agency has issued security training mandates for rail workers and urges DHS to "address this problem by immediately issuing training standards and requirements." To my knowledge, the Department has not yet responded to this letter and DHS and TSA still has not mandated that passenger rail agencies provide security training to employees as a condition of receiving security grants. What is TSA doing to ensure front line rail employees are receiving security training?

Answer. TSA has issued two rail security directives (SD RAILPAX–04–01 and SD RAILPAX–04–02), which require rail operators to implement various security measures. While "security training" in a specified manner or amount of time is not expressly mandated, each of these measures requires passenger rail systems to educate their personnel on security requirements and ensure their implementation through repeated advisories and guidance. Training programs and materials delivered to employees meet this responsibility.

In addition, DHS is partnering with the American Public Transportation Association (APTA) to assist its employee member organizations in developing training standards for public transportation employees. These training standards are developed in collaboration with transit industry professionals, industry experts, and professional training institutes. In addition, both the Federal Transit Administration and TSA fund and support a variety of safety and security training initiatives for transit agencies and their employees. Much of the training is available at no cost. Transit-specific training programs include recognizing terrorist activity and response, explosives incidents, weapons of mass destruction, and responding to a hijacking. For example, through the Federal Law Enforcement Training Center, TSA sponsored the Land Transportation Anti-Terrorism Training Program which has trained over 400 Law Enforcement and Transit personnel as of the end of FY05.

Question 9. During a hearing on the London bombings, you described security on the Nation's mass transit systems as "outstanding" despite the fact that TSA had not completed its security risk assessments and transit workers, like rail workers, are not being trained. How would you characterize the state of security on our railroads? What steps need to be taken to improve rail security and what is TSA doing about it?

Answer. The mass transit and rail industry, and State and local governments, are to be commended for their proactive response and significant commitments in addressing homeland security issues, both pre- and post-9/11, and following the Moscow, Madrid and London bombing incidents. The responsible government approach has been to continue to leverage these efforts as we developed baseline standards and refined our rail security strategy.

To this end, the United States Government has made significant enhancements to transportation security, specifically in rail and mass transit, and put specific measures in place after the Madrid attacks. Security standards for rail are in place; criticality and vulnerability assessments have been completed and are continuing; inspectors are being deployed across the country; and new technologies have been tested. For example, TSA took major strides in developing and field-testing a new technology, in the Transit and Rail Inspection Pilot (TRIP) for screening passengers and baggage in a rail environment for deployment during high threat scenarios. (Deployed to the Republican National Convention in August 2004 and Presidential Inauguration in January 2005 at the request of Amtrak).

Nevertheless, I recognize that improving the state of security in our Nation's transportation network and facilities is a continuing endeavor. Specific efforts that TSA is taking in the rail area include:

- continuing rail corridor assessments in high threat urban areas where Toxic by Inhalation (TIH) materials are transported;
- expanding inspections of passenger rail operations and their associated facilities for compliance with the TSA issued security directives and identification of potential security gaps, utilizing TSA's 100 rail inspectors; and
- Continuing to partner with the DHS' Science & Technology Directorate to pursue and test detection and other technologies applicable in the rail and mass transit environment.

TSA will also continue to assist system operators identify their security risks through: (1) security assessments, both government-facilitated and through use of self-assessment tools, (2) compliance efforts, and (3) through cooperative partnerships with industry associations and operators to develop effective and cost-efficient mitigation strategies.

Question 10. Does TSA have plans for more non-aviation related security requirements for the industry? If so, in what areas?

Answer. The Department of Homeland Security publishes a semiannual summary of all current and projected rulemakings, reviews of existing regulations, and completed actions of the Department of Homeland Security (DHS) and its component agencies and divisions. This agenda provides the public with information about DHS' regulatory activity, thereby enabling the public to be more aware of and effectively participate in the Department's regulatory activity. DHS made its most recent semiannual publication on October 31, 2005 (70 FR 64629). The following, relating specifically to TSA's regulatory agenda, is excerpted from the October 31, 2005 entry in the *Federal Register:*

Transportation Security Administration—Proposed Rule Stage

Sequence Number	Title	Regulation Identifier Number
1441	Aircraft Repair Station Security	1652–AA38
1442	Foreign Air Carriers	1652–AA40
1443	Transportation Worker Identification Credential (TWIC) Maritime	1652–AA41
1444	Modification of the Aviation Security Infrastructure Fee (ASIF)	1652–AA43
1445	Due Process for FAA Certificate Holders and for Other Threat Assessments	1652–AA44
1446	Registered Traveler (RT)	1652–AA47

Transportation Security Administration—Final Rule Stage

Sequence Number	Title	Regulation Identifier Number
1447	Imposition and Collection of Passenger Civil Aviation Security Service Fees	1652–AA00
1448	Aviation Security Infrastructure Fees (ASIF)	1652–AA01
1449	Air Cargo Security Requirements	1652–AA23
1450	Privacy Act of 1974: Implementation of Exemptions; Intelligence, Enforcement, Internal Investigation, and Background Investigation Records	1652–AA34
1451	Flight Training for Aliens and Other Designated Individuals; Security Awareness Training for Flight School Employees	1652–AA35
1452	Secure Flight Program	1652–AA45

Transportation Security Administration—Final Rule Stage—Continued

Sequence Number	Title	Regulation Identifier Number
1453	Technical Amendment: Administrative Organizational Changes	1652–AA46
1454	Privacy Act of 1974: Implementation of Exemptions; Secure Flight Records	1652–AA48

Transportation Security Administration—Long-Term Actions

Sequence Number	Title	Regulation Identifier Number
1455	Civil Aviation Security Rules	1652–AA02
1456	Security Programs for Aircraft Weighing 12,500 Pounds or More	1652–AA03
1457	Private Charter Security Rules	1652–AA04
1458	Background Checks for Airport Workers	1652–AA06
1459	Protection of Sensitive Security Information	1652–AA08
1460	Security Compliance Program for Aircraft Operators	1652–AA09
1461	Security Compliance Program for Airports	1652–AA10
1462	Criminal History Records Checks	1652–AA11
1463	Transportation of Explosives From Canada to the United States Via Commercial Motor Vehicle and Railroad Carrier	152–AA16
1464	Security Threat Assessment for Individuals Applying for a Hazardous Materials Endorsement for a Commercial Drivers License	1652–AA17
1465	Surface Transportation Security Directives	1652–AA26
1466	Enhanced Security Procedures for Operations at Certain Airports in the Washington, D.C., Metropolitan Area Flight Restricted Zone	1652–AA39
1467	Ronald Reagan Washington National Airport: Enhanced Security Procedures for Certain Operations	1652–AA49

Question 11. The recent GAO report on passenger rail security (GAO–05–851) questions the feasibility of enforcing the TSA security directive issued to passenger rail operators following the Madrid bombings in May 2004. Are the May 20, 2004 passenger rail security directives enforceable? Does TSA have penalty authority with regards to non-aviation security directives? Has TSA issued fines against any passenger rail operator or owner for noncompliance?

Answer. The TSA Security Directives issued on May 20, 2004, are fully enforceable. TSA has available a number of enforcement mechanisms to ensure that regulated entities comply with applicable requirements. TSA may employ a variety of tools to encourage action that secures compliance, including:

- On-the-spot counseling: Minor instances of noncompliance are identified and can be immediately corrected in the presence of the inspector.
- Corrective action: Measures taken by the passenger rail system to correct a deficiency in a manner that protects against recurrences. These measures may be developed by the passenger rail system and approved by TSA, expressly prescribed by TSA, or mutually prepared by the system and TSA. Written documentation of the corrective action is made through a simple written description of measures taken to address the discrepancy or preparation of the formal written plan compliance plan.
- Compliance notice: TSA may issue a compliance notice to a passenger rail system following an inspection that reveals noncompliance with mandatory security requirements, such as the security directives. The notice requests the passenger rail system owner or operator to submit a compliance plan, describe corrective actions already taken, or dispute the allegation of noncompliance within 10 days of receipt.

TSA also possesses general authority to seek civil penalties through proceedings in Federal District Court, against any party for any violation of a TSA issued standard, regulation, or requirement. Under 49 U.S.C. 46305, a civil penalty “may be collected by bringing a civil action against the person subject to the penalty, a civil action in rem against an aircraft subject to a lien for a penalty, or both.” Pursuant to 49 U.S.C. 46301(a)(4), the maximum penalty available for non-aviation security related violations is $10,000. Initiating any proceeding in Federal District Court requires the concurrence and assistance of the Department of Justice. To date, TSA has not initiated any enforcement action through Federal District Court proceedings. TSA may seek and impose civil penalties for alleged violations of aviation security standards through an administrative proceeding (unless certain statutory exclusions under 49 U.S.C. 46301(d) apply). However, TSA requires additional authority from Congress to seek and impose civil penalties for alleged violations of surface security standards through an administrative proceeding.

Question 12. The results of the Teamsters Rail Security Report released on September 29, 2005, are very distressing. Sixty-eight percent of the respondents of the survey saw trespassers in the rail yard on the date the survey was taken, and 96 percent responded that there was no security presence in the yard that day. Additionally, 84 percent of the respondents stated they had received no additional training relating to terrorism prevention in the last twelve months, and 62 percent responded they had not been trained in the railroads' emergency action or response plan. Has TSA issued any security directives that address these security problems? If so, does TSA intend to enforce them? If not, are such security directives being put under consideration?

Answer. TSA issued rail security directives in May 2004 (SD RAILPAX–04–01 and SD RAILPAX–04–02). In crafting the security directives, TSA required rail operators to take steps to provide for the physical security of rail facilities, such as rail yards. Among other things, rail operators are required to ensure that their personnel are notified through various media of changes in threat conditions, reinforce employee watch programs, and ensure that employees maintain vigilance and immediately report through the appropriate chain of command any situation that constitutes a potential threat or suspicious activity. Additionally, the systems are required to inform passengers of heightened security measures and the need to be vigilant and report suspicious activity. While "security training" in a specified manner or amount of time is not expressly mandated, each of these measures requires passenger rail systems to educate their personnel on security requirements and ensure their implementation through repeated advisories and guidance. Training programs and materials delivered to employees meet this responsibility.

In addition, DHS is partnering with the American Public Transportation Association (APTA) to assist its employee member organizations in developing training standards for public transportation employees. These training standards are developed in collaboration with transit industry professionals, industry experts, and professional training institutes. In addition, both the Federal Transit Administration and TSA fund and support a variety of safety and security training initiatives for transit agencies and their employees. Much of the training is available at no cost. Transit-specific training programs include recognizing terrorist activity and response, explosives incidents, weapons of mass destruction, and responding to a hijacking. For example, through the Federal Law Enforcement Training Center, TSA sponsored the Land Transportation Anti-Terrorism Training Program which has trained over 400 Law Enforcement and Transit personnel as of the end of FY05.

As indicated in the response to question #11, TSA possesses a variety of enforcement tools to elicit compliance with the security directives.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO EDMUND "KIP" HAWLEY

Question 1. What is your agency doing to ensure that front line rail employees—the eyes and ears of the railroad environment—are receiving appropriate security training?

Answer. The Transportation Security Administration (TSA) has issued two rail security directives (SD) (SD RAILPAX–04–01 and SD RAILPAX–04–02), which require rail operators to implement various security measures. While "security training" in a specified manner or amount of time is not expressly mandated, each of these measures requires passenger rail systems to educate their personnel on security requirements and ensure their implementation through repeated advisories and guidance. Training programs and materials delivered to employees meet this responsibility.

Through the Annex to the Interdepartmental DHS and DOT MOU the Office for Domestic Preparedness is partnering with the FTA to determine and deliver where appropriate cross discipline training programs designed to enhance the awareness, and ability to prepare for, respond to, and recover from an incident. In addition, DHS is partnering with the American Public Transportation Association (APTA) to assist its member organizations in developing training standards for public transportation employees. These training standards are developed in collaboration with transit industry professionals, industry experts, and professional training institutes. In addition, both the Federal Transit Administration and TSA fund and support a variety of safety and security training initiatives for transit agencies and their employees. Much of the training is available at no cost. Transit-specific training programs include recognizing terrorist activity and response, explosives incidents, weapons of mass destruction, and responding to a hijacking. For example, through the Federal Law Enforcement Training Center, TSA sponsored the Land Transportation Anti-Terrorism Training Program which has trained over 400 Law Enforcement and Transit personnel as of the end of FY05.

Question 2. By law, the Secretary of Transportation—or his designee—sits on the Amtrak board of directors. In April, the board approved Amtrak's funding request for Amtrak's security needs of up to $254 million a year (figure includes "support" functions as well). If this funding was needed to help secure Amtrak and its 25 million annual passengers, why didn't President Bush ask for it in his budget?

Answer. The Transportation Security Administration (TSA) believes that this question would most appropriately be directed to the Department of Transportation, since Amtrak funding is within its purview.

Additionally, the Department of Homeland Security's Office of State and Local Government Coordination and Preparedness (SLGCP) has provided $6,373,730 in grant funding to Amtrak in FY 2005 for security enhancements for intercity passenger rail operations in the Northeast Corridor (service between Washington, D.C. and Boston, Massachusetts) and at Amtrak's hub in Chicago, Illinois. In addition, a further $726,270 in technical support is being provided to Amtrak in FY 2005 through the SLGCP Mass Transit Technical Assistance Program. This support will entail a facilitated risk assessment of Amtrak's Northeast Corridor and Chicago operations designed to provide Amtrak with a risk management strategy and roadmap for making funding allocation decisions on security enhancements to the most critical portions of its system.

Question 3. Will the Administration specifically request funding for Amtrak's security needs in FY07?

Answer. Again, the Transportation Security Administration (TSA) believes that this question would most appropriately be directed to the Department of Transportation, since Amtrak funding is within its purview. TSA fully integrates Amtrak into all of our security planning and is working to further enhance information and intelligence sharing capabilities.

Question 4. How would you characterize the state of security on our railroads?

Answer. The mass transit and rail industry, and State and local governments, are to be commended for their proactive response and significant commitments in addressing homeland security issues, both pre- and post-9/11, and following the Moscow, Madrid and London bombing incidents. The responsible government approach has been to continue to leverage these efforts as we developed baseline standards and refined our rail security strategy.

To this end, the United States Government has made significant enhancements to transportation security, specifically in rail and mass transit, and put specific measures in place after the Madrid attacks. Security standards for rail are in place; criticality and vulnerability assessments have been completed and are continuing; inspectors are being deployed across the country; and new technologies have been tested. Federal efforts have focused on greater information sharing between the industry and all levels of government, addressing vulnerabilities, developing new security measures and plans, increasing training and public awareness campaigns, and providing greater assistance and funding, mostly in the form of security grants, to help ameliorate the cost borne by the non-federal stakeholders.

Following both July incidents in London, Transportation Security Administration (TSA) surface transportation security inspectors were deployed to operations centers for passenger rail and mass transit systems. Those inspectors were supplemented by Federal Railroad Administration inspectors. Working together, they found the systems had initiated actions to ensure compliance with security requirements and swiftly implemented enhanced security measures, even before the Department of Homeland Security (DHS) had raised the threat level for mass transit to Orange.

Of note, the Federal Transit Administration (FTA) reported that as of August 2005 some 90 percent of the Nation's top 50 transit systems were in full compliance with its Top 20 Security Program Action Items for Transit Agencies. FTA developed this list following the 9/11 terrorist attacks and has regularly monitored compliance with these guidelines. TSA will continue to build upon this frame work as it utilizes a threat-based, risk-management approach to continually focus resources, as needed, to ensure the security of the Nation's transportation system and its critical infrastructure.

Question 5. What is TSA doing to track high-hazmat rail cars?

Question 6. Does the Administration believe that active monitoring of the movement of high-hazmat rail cars is necessary?

Answer to Questions 5 and 6. There is no class of materials classified as "high hazmat" in Federal law or regulation. The Transportation Security Administration (TSA) is currently studying the feasibility and value of actively monitoring rail cars that carry materials that are Toxic by Inhalation (TIH). The study will encompass both testing of available technology, cost and the development of systems to allow for third-party tracking of rail car movements. At present, the rail industry has the ability to track these TIH shipments using existing technology that has been established for commercial and operational purposes. TSA is studying enhanced technologies to supplement the current method of tracking rail cars. It is envisioned that these enhanced technologies may provide more accurate real-time location tracking and provide additional data such as product releases and container tampering. TSA is also considering what level of threat will require active monitoring and the value of the data generated by active monitoring.

In addition, the Department of Homeland Security (DHS) and the Department of Transportation (DOT) have been working on various initiatives that support the development of a national risk-based plan to address the shipment of hazardous materials by rail and truck. For rail, DHS and DOT are focusing on the assessments of vulnerabilities of high threat urban areas where TIH are transported, identification of practical alternatives to placards on rail tank cars, new rail car design standards, and the development of hazardous materials security plans to improve the adequacy and effectiveness of industry security plans. Through the FY 2005 TSGP, the Office for Domestic Preparedness provided $5,000,000.00 for three projects designed to enhance the security of TIH corridors. The three projects are:

1) Development of a Rail Corridor Risk Management Tool;
2) Development of a Rail Corridor Hazmat Response and Recovery Tool; and
3) Development and demonstration of "Save Haven" concepts for in-route toxic inhalation hazard shipments.

These projects were made available and are being managed by the Office for Domestic Preparedness as identified through partnerships with other DHS entities, including TSA, the Border and Transportation Security Directorate, and the Information Analysis and Infrastructure Protection Directorate, as well as with the Federal Railroad Administration and the Pipeline and Hazardous Materials Safety Administration within the Department of Transportation. These projects offer the potential for long-term enhancement of freight rail security.

Question 7. Assuming the Federal Government is able to collect vital information about hazmat releases, how will it distribute this data to first responders who may be putting their own lives at risk just by arriving on scene?

Answer. Measures are in place to provide state and local governments, and by extension first responders, sufficient information to protect their communities in the event of an accident or an attack involving hazmat releases. The Department of Homeland Security (DHS) and the Transportation Security Administration (TSA) currently provide notification to municipalities on the pending movement of hazardous materials through local jurisdictions on a case-by-case basis. DHS/TSA believes that case-by-case notification is sufficient and that in otherwise normal circumstances comprehensive real-time notification is not warranted. For example, here in Washington, D.C., for special events such as the Fourth of July and President Reagan's funeral, local governments were provided information in advance of hazardous materials shipments passing through the local jurisdictions in this area. In such rare cases, information provided to local jurisdictions can be analyzed by the governments in light of the risk and threat to determine whether additional measures are necessary. In addition, rail carriers annually provide the governments with a picture of the types and quantities of the hazardous materials that have come through the jurisdiction. This information enables the governments to prepare, plan, and train for any incident involving a hazardous material that is typically transported through their jurisdictions.

As noted in question 6 above, the vision for the Development of a Rail Corridor Hazmat Response and Recovery Tool would be to improve response by providing first responders with the appropriate tools, equipment, and training for responding to a major freight rail incident.

Following the terrorist attacks on September 11, concerns were raised that placards may unduly draw attention to the transport of hazardous materials on rail cars. On July 25, 2003, TSA coordinated and hosted a Placard Workshop to enable industry and first responder representatives to discuss with TSA the issues surrounding the potential removal of placards on rail cars. As a result of the Placard Workshop, TSA was requested to conduct an independent study, and it contracted with the Texas Transportation Institute (TTI) to determine whether there are feasible alternatives to the current rail placarding system. The comprehensive study examined the available technology, and input from first responders, rail operators and other key stakeholders was included. As a result of the findings of the study, Secretary Chertoff announced on April 7, 2005, that the Department was recommending continuation of the placard system for hazardous materials transported by rail, which is designed to ensure the safety of citizens and first responders.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO EDWARD WYTKIND

Question 1. As the representatives of the major sectors of the railroad industry, you live with the challenges of securing your railroads everyday. We have tried to craft a bill that will help make this job easier. Yet, I'm sure we can do more. Can you tell us which of our provisions you feel are most needed and why? If there were one thing more we could do in this bill to help you reach your goal of a safe and secure railroad and workplace, what would it be?

Answer. As explained in my submitted written statement, Section 310, the Rail Worker Security Training Program, is extremely important and will from our perspective make important improvements to rail security. Training is relatively inexpensive and experts have confirmed that a well prepared and informed workforce can help prevent a terrorist attack and mitigate harm if one does occur. As far as improvements that we would like to see, we continue to believe the whistleblower protections need to be enhanced to ensure that workers are not discouraged or intimidated from reporting security concerns.

Question 2. From listening to your testimony and the statements of other witnesses at the hearing, there seems to be some disconnect between what we have heard and the perception from the vantage point of the rail worker. Based on the Teamsters Rail Security Report released on September 29, 2005 and your testimony, we learned that rail workers are not receiving the training they need to do their jobs effectively, and that there is too often open access to facilities where an ill-intentioned person could do significant harm. Can you provide more information concerning what your members are seeing everyday and what we can do about it?

Answer. We agree that there is a disconnect between what industry is reporting and our perspective on what is actually happening on the ground. I should note that my observations are based on conversations we have had with local leaders and rank-and-file workers. These are the employees who are on the front lines and understand their railroad property and its vulnerabilities as well as know first-hand how little is being done to deal with security risks. Specifically, our members report that rail facilities, tracks and other infrastructure are not being adequately protected or secured. Credentials are not being fully used and there is potential for unauthorized individuals to enter facilities. In addition, and as explained in more detail below, security training is sorely lacking.

Question 3. Are you familiar with the survey, discussed above, of rail workers regarding rail security efforts undertaken by the Brotherhood or Locomotive engineers and Trainman that found that workers do not feel adequately trained to address a rail security incident? Do you believe that these findings are generally consistent with the situation facing the employees that you represent?

Answer. While we cannot speak to the specifics of the survey, we can report that the findings are generally consistent with the situation that is faced by the employees represented by TTD unions.

Question 4. Can you explain some of the benefits of consistent worker training standards, and why from the perspective of your members a Federal mandate is needed?

Answer. Workers need to know how to identify a security risk, what to do in response, and the steps that must be taken in the event an attack does occur. While we understand that not all workers need the same training, without Federal standards and guidelines that carriers must follow, our experience is that the content of training will be highly deficient. Furthermore, if training is left to the discretion of individual carriers, we know that too often carriers will opt not to provide training across the board. Safety and security should not vary from carrier to carrier - we must have one level of security throughout the system. Simply put, a mandate is needed because without it the status-quo will remain in effect and that is simply not acceptable.

Question 5. Do you know what percentage of the front-line rail employees that you represent have received any security training?

Answer. We do not currently have that data for our members. It should also be noted that even if training has occurred, it is a separate question if that training is comprehensive and if recurring training is being done.

Question 6. You mentioned in your testimony, the need for more robust whistleblower protection for rail workers. What about the provision of this Committee's bill, Sec. 311 of S. 1052? What changes do you recommend to what is already provided? Are you aware of specific cases where employees have been punished for raising security concerns?

Answer. Section 311 is a good start and we supported its inclusion but we believe that improvement should be made. Specifically, the provision should follow the model of protections provided for financial whistleblowers as in the Sarbanes-Oxley Act. This law ensures that whistleblower complaints are considered in a more timely fashion and allows workers to pursue a action in Federal court if agency response is unnecessarily delayed.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO JOSEPH H. BOARDMAN

Question 1. I have worked hard, together with Chairman Stevens, to craft a solid blueprint for future Federal actions to secure our Nations' railroads. The rail provisions of S. 1052 include security upgrades, threat assessments, security training, research and development, and several other important initiatives, many of which were unanimously approved by the Senate last year. Yet, if we can strengthen our efforts, we must. I hope each of you will help us do that. What is your position on the rail provisions of S. 1052? How can we improve them?

Answer. The U.S. Department of Transportation (DOT) has worked with the U.S. Department of Homeland Security (DHS) to provide the Administration's views on S. 1052. Those views were conveyed to Chairman Stevens by letter dated November 10, 2005. We would, however, like to point out some additional issues with S. 1052 that should be considered.

Sec. 304. Fire and Life-Safety Improvements

This section would authorize a total of $670 million for FY 2006–2008 to be made available to the Secretary of Transportation, from funds appropriated under section 102 of the bill to the Secretary, to make grants to Amtrak for design and construction of fire- and life-safety improvements to tunnels in New York, New York; Baltimore, Maryland; and Washington, D.C. Funds appropriated pursuant to this section would remain available until expended. Amtrak would be required to submit for the Secretary's approval an engineering and financial plan for projects and a project management plan for each project. The Secretary would not be authorized to disburse funds to Amtrak unless the Secretary had approved such plans. The section would also establish a complex series of deadlines for the Secretary's review of the plans.

DOT opposes this provision as an unnecessary infringement on the Secretary's discretion to carry out the review of Amtrak's plans. DOT recognizes the benefits of fire- and life-safety improvements to these critical elements of the Nation's rail infrastructure. In recognition of the importance of these tunnels, not just for intercity but also for commuter rail service, we believe that any funds made available for this purpose should flow through a Federal-State partnership such as that proposed in the Administration's April 13, 2005 legislative proposal to restructure intercity rail passenger service—the Passenger Rail Investment Reform Act.

Sec. 315. Welded Rail and Tank Car Safety Improvements

This section would mandate that FRA undertake certain actions to improve the safety of railroad track and railroad tank cars.

There does not appear to be a need for this legislation because a very similar provision was enacted in August 2005 as section 9005 of the Safe, Accountable, Flexible, and Efficient Transportation Equity Act of 2005 (SAFETEA–LU, Pub. L. 109–59).

Sec. 316. Report Regarding Impact on Public Safety of Train Travel Communities Without Grade Separation

This section would require that DOT, in consultation with the Transportation Security Administration (TSA) and State and local governments, study and report to Congress on the effect of blocked highway-rail grade crossings upon the ability of emergency responders to perform public safety and security duties.

There does not appear to be a need for this legislation as a similar provision was enacted in section 9004 of SAFETEA–LU.

Question 2. The FRA issued a Safety Advisory earlier this month calling on railroads that transport hazardous materials to improve procedures for tracking the movement of time-sensitive shipments. The advisory also emphasized that all railroad employees who handle such shipments be aware of, and clearly understand, the procedures. The Advisory was issued as a result of an incident that occurred in Cincinnati this summer, when a tank car carrying styrene sat idle on the same railroad for seven months and as a result of the long delay, exploded. Such negligence poses obvious security risks. What is the FRA doing to ensure compliance with these new requirements, including employee awareness? What additional steps has the FRA taken to secure the movement of hazardous materials by rail?

Answer. FRA issued Safety Advisory 2004–05 on September 29, 2005, to improve the safety and reliability of hazardous materials shipments by railroad. The Safety Advisory informs shippers, consignees, and railroads of the dangers of allowing cars of time-sensitive chemicals to remain undelivered beyond their anticipated date of placement, and recommends enhanced procedures to avoid such occurrences. While FRA cannot enforce compliance with the Safety Advisory, as it does not impose any requirements in itself, FRA is closely monitoring the industry's efforts to promote the timely shipment of time-sensitive hazardous materials in accordance with the recommendations in the Safety Advisory. FRA is also closely monitoring the compliance of railroads, shippers, and consignees with existing DOT regulations, which require notification and special awareness for those time-sensitive materials posing a significant risk in transportation. FRA will pursue future regulatory or other action should the Safety Advisory and existing regulations prove insufficient to minimize the safety risks associated with the movement of time-sensitive hazardous materials.

FRA recognizes that employee awareness and understanding of the regulations and procedures governing the safe transport of time-sensitive hazardous materials shipments are critical, and DOT regulations at 49 CFR 172.700 et seq., provide for initial and recurrent training of all employees engaged in the transportation of hazardous materials. Railroads also impose additional training requirements, and FRA expects that this Safety Advisory will be made a part of the industry's hazardous materials transportation training curriculum.

FRA has taken additional steps to promote the safety and security of the movement of hazardous materials by rail. On October 24, 2005, FRA issued Emergency Order No. 24, which requires railroads to modify their operating rules and take other action necessary to ensure that railroad employees who dispatch non-signaled territory or who operate hand-operated main track switches in non-signaled territory restore the switches to their proper (normal) position after use. The failure to restore such switches to their proper position after use has resulted in a number of accidents and fatalities. This Emergency Order is part of a broader focus on human factor-caused train accidents that is being conducted under the auspices of FRA's Railroad Safety Advisory Committee (RSAC). RSAC has tasked its Operating Rules Working Group to develop recommendations to reduce human factor-caused train accidents generally, and the Working Group is scheduled to report its findings and recommendations to the full RSAC in February 2006.

FRA also has ongoing a number of additional initiatives to promote and enhance the safety and security of hazardous materials shipments. Since January 2004 FRA has inspected more than 3,600 security plans (including the plans for all the major rail carriers) and reviewed the training records for more than 29,000 rail hazmat employees. As a result, we are processing 120 recommended civil penalty actions for violations of the DOT security regulations. DOT and DHS are examining the feasibility of specific security enhancements, including improvements to security plans, modifications of methods used to identify shipments, enhanced requirements for temporary storage, strengthened tank car integrity, and implementation of tracking and communication systems. FRA staff have also provided support to the vulnerability assessments led by TSA on several rail corridors.

FRA and DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA) are also coordinating with DHS in formulating proposed regulations that would enhance the current security plan requirements, as a follow-up to an August

16, 2004, notice (jointly issued by PHMSA and TSA). Possible enhancements under consideration include data collection on shipments of Toxic Inhalation Hazard (TIH) and other highly hazardous materials; analysis of safety and security risks along rail transportation routes where these materials are transported; alternative routing options; and en route storage.

Question 3. Are there plans to cross-train FRA and TSA rail inspection staff so that when conducting inspections, both sets of inspectors can be looking for safety and security problems? What do you think of the concept of creating a unified Federal rail inspection team to ensure maximum efficiency and coordination, rather than having separate TSA and FRA inspectors essentially performing the same function separately?

Answer. There are generally no plans to cross-train FRA and TSA rail inspection staff so that both sets of inspectors look for both safety and security problems. Instead, FRA has been working closely with the managers of TSA's new inspection program to ensure that the roles of the two agencies' inspectors are clearly distinguished and do not result in duplicative inspections of the rail industry. FRA's safety mission is critical and requires the constant attention of its inspection force. FRA believes that public safety is best served by having FRA inspectors direct their expertise in monitoring compliance with the extensive body of laws and regulations governing the five major areas of railroad safety: track, signal systems, equipment, operating practices, and hazardous materials shipments.

FRA does not believe that uniting TSA and FRA inspectors into a single, Federal rail inspection team would ensure maximum efficiency and coordination, as the question suggests, as TSA and FRA rail inspectors generally do not perform the same functions. For example, TSA rail inspectors are focused on securing the rail transportation network from terrorist attack through the evaluation of potential terrorist targets, identification and elimination/neutralization of security gaps, identification of suspicious persons and objects, and more—functions which are generally distinct from those performed by FRA safety inspectors.

Of course, FRA's railroad safety mission necessarily includes involvement in railroad security issues and, in those areas such as hazardous materials transportation where safety and security are significantly interrelated, FRA inspectors will continue to have an active role. FRA has been and will continue to be engaged in the railroad industry's response to the threat of terrorism, as detailed in Administrator Boardman's written testimony. Yet, FRA believes that through careful delineation of that role, and close coordination with TSA, FRA's security efforts will dovetail with those of TSA while continuing to allow FRA to keep its principal focus on railroad safety.

Question 4. I understand that the FRA and TSA have been working on a rail security annex to the MOU developed between the Department of Transportation and the Department of Homeland Security. S. 1052 requires the agencies to complete this annex within one year following enactment. Can you tell us what the current status of this rail security annex is?

Answer. FRA has prepared an annex addressing rail security issues, including relations between FRA inspectors and TSA's new inspection workforce. FRA has shared the draft annex with TSA, and we hope that it will be completed soon.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO JOSEPH H. BOARDMAN

Question 1. What additional enforcement action is the Federal Railroad Administration taking to ensure railroads and hazmat shippers are complying with your recent safety advisory on rail hazmat transportation?

Answer. Please see the answer to Question 2 from Senator Inouye. The answer addresses this question and provides additional information.

Question 2. Is rail transportation of high hazmat and handling incident thereto inherently dangerous?

Answer. Rail transportation and handling of any hazardous material, especially TIH materials, are dangerous when not properly done. Congress recognized this very danger long ago and has regulated these activities. Over the years, a body of statutory law and detailed administrative regulation has been developed to address the risks associated with the transportation and handling of hazardous materials. FRA and DOT as a whole continually seek ways to further mitigate these risks, such as through efforts to enhance the security of TIH shipments. The effectiveness of this regulatory regime is evidenced by the remarkably low number of incidents in light of the high volume and length of haul of TIH materials transported by rail.

Question 3. Does it present a safety or security risk?

Answer. By definition, hazardous materials pose various types of risks to safety, including security. Under DOT's hazardous materials transportation regulations, there are nine designated classes of hazardous materials, most of which are further subdivided by specific hazard. See 49 CFR 173.2. As noted above, DOT's promulgation and enforcement of these regulations help to manage the risks posed, and we continually seek ways to further mitigate these risks.

Question 4. By law, the Secretary of Transportation—or his designee—sits on the Amtrak board of directors. In April, the board approved Amtrak's funding request for Amtrak's security needs of up to $254 million a year (figure includes "support" functions as well). If this funding was needed to help secure Amtrak and its 25 million annual passengers, why didn't President Bush ask for it in his budget?

Answer. FRA does not believe it correct to characterize the $254 million figure as a funding request, *per se.* Rather, this amount was for use as an internal budgeting threshold. Funding for Amtrak's police and security needs would come from Amtrak's operating funds, up to this dollar amount, as determined by Amtrak's management. Further, the President's budget for FY06 had already been submitted to Congress by April 2005.

Question 5. Will the Administration specifically request funding for Amtrak's security needs in FY07?

Answer. The President's FY07 budget request has not yet been finalized. As a result, it would be premature to discuss what specific initiatives will be in that request. We will be glad to share with the Committee the details of the FY07 budget request, once we are in a position to do so.

○