COMMITTEE PRINT: RAIL AND PUBLIC TRANSPORTATION SECURITY ACT OF 2007

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

MARCH 6, 2007

Serial No. 110–12

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

35–271 PDF WASHINGTON : 2009

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California,
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
VACANCY

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
BOBBY JINDAL, Louisiana
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*
TODD GEE, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

CONTENTS

COMMITTEE PRINT: RAIL AND PUBLIC TRANSPORTATION SECURITY ACT OF 2007

Tuesday, March 6, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
WASHINGTON, DC.

The committee met, pursuant to call, at 10:09 a.m., in Room 311, Cannon House Office Building, Hon. Bennie Thompson [chairman of the committee] presiding.

Present: Representatives Thompson, Markey, Harman, Norton, Lofgren, Etheridge, Langevin, Cuellar, Carney, Clarke, King, Shays, Lungren, Rogers, Reichert, Dent, Bilirakis, and Davis of Tennessee.

Mr. THOMPSON. [Presiding.] The Committee on Homeland Security will come to order.

The committee is meeting today to receive testimony on the committee print entitled, "Rail and Public Transportation Security Act of 2007."

Like all Americans, I am alarmed at the lack of security for rail and public transportation systems around the country. Each weekday 11.3 million passengers in 22 states use commuter heavy and light rail. History has shown that terrorists view rail and public transportation systems as potential targets.

This coming Sunday will be the 3-year anniversary of the terrorist bombing of Madrid rail system, which killed and maimed hundreds of innocent civilians. This coming July marks the second anniversary of the terrorist bombing throughout London's public transportation system. Last summer, a number of bombs tore through Mumbai's system. Just last month, a passenger train outside New Delhi caught fire when suitcases filled with flammable liquid were exploded as the train headed for Pakistan.

Despite all of these attacks, rail and public transportation security remains a secondary issue to aviation security. The 9/11 Act that Congress passed in 2004 directed TSA to develop a national strategy for transportation security. TSA produced a document, but it was not a comprehensive strategy.

The President directed the Department of Homeland Security to complete a transportation sector specific plan more than 3 years ago. This plan has yet to be completed.

Last December, the president issued an executive order directing the Department of Homeland Security to strengthen surface transportation security. Yet in the fiscal 2008 budget, the president only requested an additional $4 million for TSA's surface transportation budget.

TSA's entire surface transportation budget is less than 1 percent of the president's requested for aviation security. Similarly, I am concerned about the money the President has requested for rail and public transportation security grants. $175 million for rail and public transportation security grants is not enough money when one considers the millions of men and women who use these systems daily.

I am also concerned about the lack of training for frontline rail and public transportation workers. Labor organizations say that their members are not being given the training to respond to acts of terrorism. According to the National Transit Institute, only about 30 percent of the transit employee workforce has received the proper training developed by the NTI and federal agencies. Shouldn't mandatory training for our frontline workers be mandatory and ongoing?

I am also worried about security issues surrounding the transportation of hazardous material. In a survey completed by the Teamsters last year, rail workers reported that equipment and HAZMAT shipments were left unattended and unsecured. Additionally, dangerous HAZMAT shipments still passed through populated areas even when alternative routes is feasible.

I know that DHS and DOT have issued proposed regulations that address some of these HAZMAT issues. But I am worried they do not go far enough. It is as though the Administration is waiting for the worst-case scenario before taking aggressive action. Well, the Committee has taken action.

We have been working on a bipartisan basis to develop the Rail and Public Transportation Security Act of 2007. I appreciate subcommittee Chairwoman Jackson Lee marking up a draft of this bill last week. And I appreciate the cooperation we have received from the minority to date. This bill will require rail and public transportation systems to complete security plans and vulnerability assessments. Right now these plans are only completed on a voluntary basis.

The bill will also mandate training for frontline rail and public transportation system employees. It will also give them whistleblower protections to encourage reporting of security risks. Thanks to an amendment offered by Representative Perlmutter and Jackson Lee, the bill also provides a redress process for employees who are terminated as a result of a background check. This bill will also make security grants available to rail, transit and bus systems.

Finally, the bill will make substantial investments in the research and development we need to find new ways to secure these systems. My hope is that through these provisions this bill will address most of the glaring gaps that currently exist in surface transportation security.

I look forward to working with my colleagues on this committee in getting this bill passed as soon as possible. Let me say that negotiations on this bill are continuing with Chairman Oberstar and the Transportation and Infrastructure Committee.

I thank each of you for coming here today. I look forward to hearing your thoughts about this proposed legislation.

VerDate Nov 24 2008 14:16 May 21, 2009 Jkt 000000 PO 00000 Frm 00006 Fmt 6633 Sfmt 6633 H:\DOCS\110-HRGS\110-12\35271.TXT HSEC PsN: DIANE

The chair now recognizes the ranking member of the full committee, the gentleman from New York, Mr. King, for an opening statement.

PREPARED STATEMENT OF HON. BENNIE G. THOMPSON

March 6, 2007 (WASHINGTON)—Today, Committee on Homeland Security Chairman Bennie G. Thompson (D–MS) delivered the following prepared remarks for the full Committee hearing on the Committee Print entitled "Rail and Public Transportation Security Act of 2007":

Like all Americans, I am alarmed at the lack of security for rail and public transportation systems around the country. Each weekday, 11.3 million passengers in 22 states use commuter, heavy, or light rail. History has shown that terrorists view rail and public transportation systems as potential targets.

This coming Sunday will be the three-year anniversary of the terrorist bombings of Madrid's rail system, which killed and maimed hundreds of innocent civilians. This coming July marks the second anniversary of the terrorist bombings throughout London's public transportation system. Last summer, a number of bombs tore through Mumbai's rail system. Just last month, a passenger train outside New Delhi caught fire when suitcases filled with flammable liquids were exploded as the train headed for Pakistan.

Despite all of these attacks, rail and public transportation security remains a secondary issue to aviation security.

The 9/11 Act that Congress passed in 2004 directed TSA to develop a National Strategy for Transportation Security. TSA produced a document, but it was not a comprehensive strategy.

The President directed the Department of Homeland Security to complete a Transportation Sector Specific Plan more than 3 years ago. This plan has yet to be completed.

Last December, the President issued an Executive Order directing the Department of Homeland Security to strengthen surface transportation security. Yet, in the fiscal year 2008 budget, the President only requested an additional 4 million dollars for TSA's surface transportation budget.

TSA's entire surface transportation budget is less than 1% of the amount the President requested for aviation security. Similarly, I am concerned about the money the President has requested for rail and public transportation security grants. 175 million dollars for rail and public transportation security grants is not enough money when one considers the millions of men and women who use these systems daily.

I am also concerned about the lack of training for front-line rail and public transportation workers. Labor organizations say that their members are not being given the training to respond to acts of terrorism. According to the National Transit Institute (NTI), only about 30% of the transit employee workforce has received the proper training developed by the NTI and federal agencies. Shouldn't training for our frontline workers be mandatory and ongoing?

I am also worried about security issues surrounding the transportation of hazardous materials. In a survey completed by the Teamsters last year, rail workers reported that equipment and HAZMAT shipments were left unattended and unsecured. Additionally, dangerous HAZMAT shipments still pass through populated areas, even where an alternative route is feasible. I know DHS and DOT have issued proposed regulations that address some of these HAZMAT issues, but I am worried they do not go far enough.

It is as though the Administration is waiting for the worst case scenario before taking aggressive action.

Well, this Committee has taken action. We have been working on a bipartisan basis to develop the "Rail and Public Transportation Security Act of 2007." I appreciate Subcommittee Chairwoman Jackson-Lee marking up a draft of this bill last week, and I appreciate the cooperation we have received from the Minority to date.

This bill will require rail and public transportation systems to complete security plans and vulnerability assessments. Right now these plans are only completed on a voluntary basis. The bill will also mandate training for frontline rail and public transportation system employees. It will also give them whistleblower protections to encourage reporting of security risks. Thanks to an amendment offered by Representatives Perlmutter and Jackson-Lee, the bill also provides a redress process for employees who are terminated during a background check.

The bill will also make security grants available to rail, transit, and bus systems.

Finally, the bill will make substantial investments in the research and development we need to find new ways to secure these systems.

My hope is that through these provisions, this bill will address most of the glaring gaps that currently exist in surface transportation security. I look forward to working with my colleagues on this Committee in getting this bill passed as soon as possible. Let me also say that negotiations on this bill are continuing with Chairman Oberstar and the Transportation and Infrastructure Committee. In the past, jurisdictional disputes have prevented good bills that would improve national security from passing Congress. Chairman Oberstar and I are committed to working together to produce a bill that will strengthen rail and public transportation security.

Mr. KING. Thank you, Chairman Thompson. And let me at the outset commend you for pushing this legislation forward. I agree with you that much more has to be done regarding rail and transit security. While there may be some differences in this legislation, I think these are differences of degree. And I am confident by the time the process is completed we should be in virtual agreement. And I want to thank you for your leadership on this issue.

It is an issue of particular importance to New York. We saw it in Madrid. We saw it in London, the absolutely deadly impact of rail bombings, the impact they can have, devastating results from them. In New York City alone we have more than 450 subway stations, probably almost 2,000 exits and entrances to those stations. In addition to that, we have commuter lines. There are literally millions of people every day on the New York City subway and commuter lines.

So this is an issue of tremendous personal impact. To any of those such as myself and Congresswoman Clark from New York who are realizing day in and day out the threat that faces our constituents. But it is a national issue. I don't want to regionalize it. I just want to show the personal impact it has on us in New York.

But I am sure that the gentlelady from the District of Columbia and certainly anyone from Los Angeles, Chicago—we can go through the whole litany of what a threat this is. And I know that Commissioner Falkenrath is here today from the NYPD's counterterrorism bureau. He will be able to testify, you know, with expertise on it. But it is a very, very real issue.

So, Mr. Chairman, I look forward to working with you on this legislation. I must though raise one issue which does have me concerned. That is the issue of how the grant funding will be administered.

I think it is absolutely essential that this committee and the Department of Homeland Security continue to have jurisdiction over the administration of grant funding for rail and transit security. And I don't say that as part of any turf battle with another committee or anything else.

The fact is whether it is the 9/11 Commission or it is outside experts, everyone agrees that as much as possible we must centralize control over homeland security issues to one committee and obviously to the committee and to the Department of Homeland Security. And to be spreading that out, to be diluting that authority, to me, will dramatically hurt the Department of Homeland Security. It will certainly decrease the jurisdiction of this committee. And besides that, it will go away from the whole idea of risk and threat-based funding that we are fighting so hard for.

So I would hope that as the process goes forward—and I know that Chairman Oberstar has legislation which would, in effect, be

giving his committee jurisdiction over that issue, we do all that we can to make sure that jurisdiction stays with this committee and ultimately that the Department of Homeland Security retains the power and the authority to distribute grants for rail and transit security.

So with that, I look forward to working with you. I thank you for the truly bipartisan effort that has gone into this. And I yield back the balance of my time.

Mr. THOMPSON. Thank you very much. I can assure the ranking member that your comments about the jurisdiction of the committee have been heard, and we have had very serious negotiations about that with T&I, and we will continue to do it. Your position and my position the same.

Other members of the committee are reminded that under the committee rules opening statements may be submitted for the record.

I welcome our first panel of witnesses.

Kip Hawley is the administrator of TSA. Mr. Hawley brings more than 20 years of transportation and technology experience to TSA.

I also want to note that Robert Jamison, the deputy administrator of TSA responsible for rail security, is here as well, sitting right behind Mr. Hawley.

And I thank both of you for being here today.

Terri Rosapep is a deputy associate administrator for program management at the Department of Transportation. He has been with the fellow Transit Administration for 5 years and has over 25 years of transportation experience at the municipal and regional level.

Welcome, sir.

Richard Fairfax is the director of enforcement at the Occupational Safety and Health Administration of the Department of Labor.

Welcome, also.

Richard Falkenrath is a deputy commissioner for counterterrorism for the city of New York Police Department. He is one of the premier scholars and leaders in homeland security issues to emerge since 9/11.

Without objection, the witnesses' full statement will be inserted into the record.

I now ask each witness to summarize his statement for 5 minutes, beginning with Mr. Hawley.

STATEMENT OF HON. KIP HAWLEY, ADMINISTRATOR, TRANSPORTATION SECURITY AGENCY, DEPARTMENT OF HOMELAND SECURITY

Mr. HAWLEY. Good morning, Mr. Chairman, members of the committee. It is a pleasure to be with you this morning to discuss TSA's work in partnership with many of the people represented here this morning in support of our nation's surface transportation systems.

I am pleased to appear today with several of our colleagues in the public and private sectors because our surface transportation security efforts are enhanced by the partnerships we have with them.

We return to these partnerships again and again because the measures they have already put in place form a very solid security foundation. Our job is built upon what has been accomplished layering additional value onto our partner security efforts.

We do that with intelligence sharing, vulnerability analysis, technology sharing, grant programs and, when appropriate, our viper teams through which TSA brings together federal air marshals, K–9 teams, and transportation security officers at the invitation of local law enforcement to provide a visible and unpredictable security presence in a variety of surface transportation environments.

TSA centers its decision making on the assessments of surface transportation. One of our fundamental principles is to take advantage of all the work done prior to 9/11, even if it wasn't originally done for security. With regard to mass transit and freight rail, we build upon the work done by the Federal Transit Administration, the Federal Railroad Administration, and other elements of the Department of Homeland Security, as well as the industry, which has conducted numerous vulnerability and readiness self-assessments.

Consistent with Secretary Chertoff's risk-based strategy for DHS, our assessments lead us to understand our vulnerabilities and direct our priorities. They lead us to focus on high-consequence risk reduction and the security fundamentals. The high-risk priorities for rail are high-density passenger transit systems in urban areas with underwater or underground tunnels and highly toxic chemicals in rail cars that are standing unattended in high-risk urban areas.

Our mitigation measures include federal grant priorities for the passenger transit systems and an innovative and immediate risk reduction approach to freight rail. In addition to the two areas mentioned, our risk assessment evaluation leads us to focus on creating visible, unpredictable, random deterrents and on raising the overall level of security, the fundamentals. The three most important fundamentals are employee training, employee preparedness and public awareness.

Employee training is the backbone of good security. And training is a top priority. We have surveyed the industry and have focused our inspectors on determining how well-trained are the frontline operators.

The results indicate, as you mentioned in your opening statement, Mr. Chairman and Mr. King, there is much work to be done. We are working aggressively to address this issue. Our plan is to take advantage of the training programs and the train the trainer programs that FTA industry and other agencies have developed.

Just last week we reissued guidance for the 2007 transit security grant program that will streamline the delivery of funding to transit agencies to get this training done. Also, we are moving toward a requirement whereby grant applicants cannot receive funding through the transit security grant program unless they demonstrate they already have the fundamentals well-covered or they gear their grant application for funds to address their deficiencies.

In 2003 and including the president's budget for fiscal year 2008, the Department of Homeland Security will make available almost $20 billion in funds that can be used to meet priority local security

needs. At the same time, DHS will make available nearly $750 million specifically targeted at mass transit security.

TSA is committed to making sure those funds translate into risk reduction and an improved security baseline.

Thank you, Mr. Chairman. I would be happy to answer your questions.

And also, I just wanted to also reintroduce Robert Jamison, who is our deputy administrator, as you mentioned, also formerly deputy administrator at FTA and acting federal rail administrator, as well as John Salmon, who has got his 30 years in the rail transportation area, who spearheads our partnership efforts. So those gentlemen are with us today, too.

[The statement of Mr. Hawley follows:]

PREPARED STATEMENT OF THE HONORABLE KIP HAWLEY

Good morning Chairman Thompson, Ranking Member King, and Members of the Committee. I am pleased to appear before you today to talk about our efforts at the Transportation Security Administration (TSA), in partnership with the Department of Transportation (DOT) and our transportation network partners, in the field of rail and surface transportation security. Many of these important security steps are built upon and fortified by a solid safety foundation that has been developed over the years by our transportation partners and DOT.

Raising the Security Baseline of an Interconnected Network

As we continue to strive to improve the security of these vital transportation systems, we must not forget the principles that make them viable and efficient. Many of these systems have been designed with mobility and ease of access as an essential component of their operational success.

These very attributes—openness, accessibility, fast-paced operations, high passenger volume—present us with our greatest security challenge.

Our efforts must work within this framework to enhance security while preserving the efficiency of these systems.

Intelligence

Non-linear risk drives everything we do. Instead of focusing on predicting the next attack, TSA takes a flexible approach and uses a risk-based methodology to address potential vulnerabilities to attack.

TSA pursues a layered approach to security in transportation, including passenger transit, highway, pipeline, and freight rail security. This approach starts by leveraging the work of United States Government entities that takes place well beyond the doors of TSA and even America's shores through effective gathering, analysis, and dissemination of intelligence. As detailed below, we do this by working collaboratively with the transportation and shipper industries, as well as with State and local officials.

The disruption of the terror plot in the United Kingdom and of the developing plot targeting underwater tunnels connecting New York and New Jersey during this past summer illustrates the necessity of this approach. The best defense is one that prevents the terrorists from ever entering the United States. TSA complements these efforts by pursuing as a strategic and operational priority the expansion of visible, unpredictable deterrence environments in our surface transportation systems to disrupt terrorists' planning and preparation activities and execution of their missions. For example, our aviation system security measures provide a significant barrier to entry for potential terrorists coming to our country. Our government's investments and improvements in terrorism watch lists, border security, and intelligence networks significantly enhance surface transportation security.

Network Approach and Strategy

To effectively address transportation security, we employ a network approach. The overall transportation system is a network. It has intersections and junctions; and while each transportation mode has its own security challenges, there are common vulnerabilities and mitigation strategies. In an effort to employ the range of security resources most effectively, we work closely with transportation networks to leverage our security impact and determine risk-based priorities.

Building on this approach, TSA implements a comprehensive strategy that applies a common methodology across all transportation networks, regardless of mode. That strategy is simple and straightforward. It consists of five elements:

- Assess industry threat, vulnerability, and consequence;
- Develop baseline security standards;
- Assess actual security status against baseline security standards;
- Develop plans to close gaps between actual status and baseline security standards; and
- Develop enhanced systems of security.

Next, let me discuss how this strategy works in practice for the freight rail, passenger rail and rail transit, highway (trucking) and pipeline industries.

Industry Threat Vulnerability and Consequence Assessments (TVC)

The purpose of threat, vulnerability, and consequence assessments is to focus efforts on and highlight risk areas. Since September 2001, many Federal agencies and industry partners have been involved in significant efforts to identify the highest risk areas for our security focus. Those efforts have centered on analyzing threats, assessing vulnerabilities, and calculating consequences of potential terrorist attacks. Based upon this large body of work and our ongoing analysis, TSA determines the areas of highest risk for each mode of transportation so that we can properly focus on risk mitigation efforts.

Freight Rail-TVC. Over the past several years, TSA has completed a number of freight rail corridor assessments in high threat urban areas. The point of the corridor assessments is to focus on high risk areas and determine the vulnerabilities. We have completed regionally based assessments in New Orleans, LA; Washington, DC; Houston, TX; Buffalo, NY; Cleveland, OH; and several cities in New Jersey including Newark, Elizabeth, and Perth Amboy. We are currently assessing Los Angeles, CA, and plan to visit additional urban areas in 2007. The results of the initial six assessments demonstrated recognizable trends and risks. We identified railcars with toxic inhalation hazard materials (TIH) sitting unattended to be a high risk potential as a terrorist target. While these shipments represent less than one percent of all rail shipments, if attacked they could create an airborne hazard and potentially endanger the lives of people living and working in those communities.

Passenger Transit-TVC. (Amtrak falls within our passenger transit division.) TSA has taken leadership in this area through a dual-track assessment initiative. Through the Baseline Assessment for Security Enhancement (BASE) program, TSA Surface Transportation Security Inspectors (STSIs) assess transit agencies' posture in 17 Security and Emergency Management Action Items encompassing a range of areas essential to an effective security program such as security and emergency management planning, risk and vulnerability assessments, implementation of random, unpredictable deterrence, training, drills and exercises, public awareness campaigns, and facility, personnel, and information security. A concurrent initiative involves transit agencies conducting self-assessments on six fundamental areas and reporting the results to TSA.

In assessing security in this area, TSA is building upon a base of knowledge derived from 37 assessments of readiness to prevent, detect, deter, and respond to terrorist incidents, conducted by the Federal Transit Administration (FTA) and the Federal Railroad Administration (FRA). The extensive field work conducted by TSA and these agencies in conjunction with the industry has been utilized to set our priorities and identify industry baseline standards. TSA and FTA/FRA assessments, in addition to in-house risk analysis, focus on passenger transit operating procedures and high risk/high consequence assets.

Highway (Trucking)—TVC. TSA has been assessing the security risks of motor carriers through the Corporate Security Review (CSR) program, another form of assessment of industry readiness and vulnerabilities. Based up on our analysis we are focused on TIH and other hazardous chemicals of concern, which include explosives, flammables and other poisonous materials.

Pipeline-TVC. Through the CSR program for pipelines, TSA has identified a number of pipeline systems that pose the highest security risk. TSA will also conduct a pipeline infrastructure study to identify the highest risk pipeline assets.

Baseline Standards

The purpose of baseline standards is to create measurable risk reduction targets.

Freight Rail Baseline Standards. Because the potential risk posed by unattended TIH rail cars in high threat urban areas was identified as the highest risk area in rail, TSA developed a risk reduction goal of reducing the objectively-measured risk of TIH cars in high threat urban areas by 25 percent per year, starting in 2007.

That risk factor takes into account car hours, the population of urban areas and the proximity to residential and commercial structures.

TSA has also identified 27 other focus areas as security action items for the rail industry to begin to address. The actions items were released to the industry in June and November 2006. The action items focus on security awareness training, security focused inspections, suspicious activity reporting, control of sensitive information and employee identification. TSA is assessing conformity with the security action items to evaluate how implementation of the action items reduces objectively measured risk.

Passenger Transit Baseline Standards. Applying the information and experience gained from extensive assessments, in-house risk analysis performed at TSA and dialogue with the industry, TSA has developed baseline standards for the industry based on six fundamental principles. Those principles are:

- Protect high risk/high consequence underground/underwater assets and systems;
- Protect other high risk/high consequence assets and systems identified in vulnerability assessments;
- Use visible, unpredictable deterrence;
- Plan and conduct awareness and response training for key personnel;
- Plan and conduct emergency drills and exercises; and
- Plan and conduct public awareness and preparedness campaigns.

Highway (Trucking) Baseline Standards. TSA has been working closely with a number of chemical shippers to develop a series of baseline security standards for both TIH and other hazardous chemicals of concern. Those standards will address specific areas such as vehicle tracking, vehicle attendance, vehicle alarm systems, truck cab access controls, locking fifth wheel on tank trailers and security route and stop areas.

Pipeline Baseline Standards. TSA has been conducting corporate security reviews targeting the top 100 pipeline operators. From the results of these reviews, TSA has developed a series of security standards based upon the best operating practices of those companies. The pipeline standards address areas including security plans, employee security training, access controls and physical access security, and employee background investigation.

Assess Security Status. The purpose of assessing security status is to determine how individual operations compare to the baseline standards. The assessment procedures vary depending upon transportation mode. Assessments in rail and passenger transit are conducted by TSA's field inspector force, while highway and pipeline assessments are conducted by TSA's subject matter experts in each network management division. The assessments are structured to target key areas of concern and to capture essential data to evaluate current practice versus baseline standards.

Freight Rail Status. In order to evaluate the security baseline in freight rail, TSA in cooperation with the rail industry is developing a comprehensive database driven system to identify the specific locations where TIH risk is the highest. TSA inspectors will verify attended/unattended status and proximity to high risk structures. In addition to identifying high risk locations, the database will give TSA the ability to identify TIH cars in near real time. This capability will allow us to more effectively respond to emerging threat situations.

Further, TSA inspectors have conducted field interviews with key rail management and personnel. Over 2,600 interviews have been completed, focused on employee security awareness, security procedures and systems to locate and protect TIH cars.

Passenger Transit Status. The results of TSA's dual-track assessment initiative have indicated variations in security posture among passenger rail and mass transit agencies. To date, 42 of the top 50 agencies by passenger volume have completed the self-assessment and reporting the results to TSA. The reports show the agencies have taken these reviews seriously. The concurrent STSI-led effort has completed in depth BASE assessments on 28 agencies in this group, driving more deeply into the specifics of security plans and procedures, operational security activities, and programs for employee security training, drills and exercises, and public awareness. Additional assessments have been scheduled, with the objective of covering all of the top 50 agencies, then moving on to agencies ranked 51 through 100. The data indicates varying security status among systems. The results are shaping TSA's strategic and operational security priorities, including security enhancement programs, grant funding, and engagement with individual passenger rail and mass transit agencies. Follow-on assessments will measure progress in improvement in the Actions Items and the fundamentals.

Highway (Trucking) Status. TSA conducts highway corporate security reviews and assessments. Those assessments are targeted at companies hauling TIH and other hazardous chemicals of concern. TSA will compare actual practice to baseline standards.

Pipeline Status. TSA will use its ongoing corporate security review process to determine the implementation of baseline standards. TSA will continue to work with individual companies to improve their security status.

Closing Gaps. Once assessments have identified the gaps in actual practice compared to baselines standards, TSA develops action plans to close the gaps and takes steps where necessary to close the gaps in all modes. We have a variety of capabilities at our disposal including industry agreements, voluntary measures, security directives, and regulatory action.

Freight Rail-Close Gaps. In order to reduce the gaps between actual practice and baseline standards, TSA pursued a two-pronged approach. We issued a Notice of Proposed Rulemaking (NPRM) on December 21, 2006, which includes several provisions to strengthen the security of the Nation's freight rail systems in the highest threat urban areas. The proposed rule establishes incident reporting procedures, codifies TSA's inspection authority, requires rail company security coordinators, and most importantly creates a positive chain of custody from beginning to end which requires secure handoffs when cars change hands.

While the proposed rule provides a number of important security initiatives, TSA believed that additional, speedier steps could be taken. As a result, we reached an agreement with the rail industry to reduce unattended TIH standstill car time in high threat urban areas beginning in early 2007. A comprehensive database will be used to identify highest priority risk reduction opportunities and working in conjunction with TSA, the rail carriers will develop site-specific action plans to reduce or remove the TIH risks. In addition to reducing the TIH risks, TSA will work with rail carriers to improve the security performance in the security training and security procedures baseline. TSA is also developing an improvised explosive device (IED) training course for rail employees to be available in the second quarter of 2007.

Passenger Transit-Close Gaps. The strategies to close security gaps start with high risk/high consequence assets.

As we know, an attack on underground, underwater, and other critical infrastructure can dramatically increase the consequences by magnifying the actual impact, complicating the response efforts and substantially prolonging the recovery time.

We must remain focused on minimizing high consequence risks. TSA, in partnership DHS's Office of Grants and Training (G&T), is leveraging the Transit Security Grant Program funds to focus on reducing risk and increasing security capabilities in State and local transit systems with the most risk. Including the President's 2008 budget, the Department of Homeland Security provided over $748 million to transit agencies and Amtrak in this pursuit.

An interagency transit tunnel risk mitigation working group has ranked this infrastructure for attention based on risk, established research and development priorities, and produced a comprehensive list of measures to guide transit agencies with this infrastructure in their security enhancement efforts. Working with the Science and Technology Directorate of DHS (S&T) and the National Laboratories, we are advancing new testing methodologies to expand our understanding of the physical effects of explosives events in transit tunnels to inform the continued development of technological solutions for risk mitigation.

While transit agencies cannot harden every entry point, nor screen every passenger coming into busy stations, they can deploy visible, unpredictable mobile teams that disrupt terrorists' planning capabilities and provide high levels of security. TSA assessments review the scope and quality of transit agencies' efforts in this area. Expanding such deterrence is a funding priority under the TSGP. TSA supplements the activities of transit agencies by expanding our canine program and leveraging our security network to create surge capacity with Visible Intermodal Protection Response (VIPR) Teams.

VIPR Teams, consisting of Surface Transportation Security Inspectors (STSIs), canine teams, Federal Air Marshals (FAMs), and advanced screening technology, provide TSA the ability to leverage a variety of resources quickly and effectively. These deployments are designed to raise the level of security in any mode of transportation across the country in heightened security environments. The teams work with local security and law enforcement officials to supplement existing security resources, provide deterrent presence and detection capabilities, and introduce an element of unpredictability to disrupt potential terrorist planning activities. More than 30 VIPR exercises have been conducted at key commuter and regional passenger rail facilities, and more are planned throughout 2007. The transition to regional plan-

ning and employment will expand the frequency of these exercises, enhancing their deterrent effect.

Explosives detection canine teams are being trained, certified, and deployed by TSA to passenger transit systems. Since late 2005, TSA's National Explosive Detection Canine Team Program (NEDCTP) has worked in partnership with passenger transit systems to train, certify, and deploy 56 explosives detection canine teams to 13 major systems in a risk-based application of resources. Forty-two of these teams are currently in place and the other 14 are projected for training, certification, and deployment in the coming months. In addition, the President's fiscal year 2008 budget proposes an additional $3.5 million to strengthen dramatically NEDCTP by approximately 45 teams to support the Nation's largest mass transit systems and expand coverage to ferry systems.

I want to emphasize that our STSI workforce and the canine teams we fund for passenger transit are just the point of the spear. There are literally thousands of transit and rail law enforcement and security officers on duty night and day to provide security where they are needed for these segments of the transportation network. Furthermore, each rail and passenger transit system makes a deliberate and strategic decision when they develop their annual budgets as to where they should apply their revenues and other funding sources to close security vulnerabilities. This approach creates a more effective network of local security rather than deploying a far greater Federal workforce to perform these same functions.

Since the security of these systems is a shared responsibility among Federal, State, and local partners, the Administration has provided significant resources to bolster these security efforts since 9/11. Funds from DHS grants programs may be used for planning, training, exercises, equipment, and other security enhancements. With the fiscal year 2007 funding, DHS will have invested nearly $18 billion in local planning, organization, equipment, training, and exercises.

In addition to visible unpredictable deterrence, TSA recognizes that training for key personnel is essential to rail as its baseline of security. There are numerous passenger transit training courses available today. Well-trained, vigilant employees provide a security force multiplier in a transit system, adding eyes and ears critical to detection and prevention. Readiness to report and respond to incidents in a timely manner can mitigate consequences and expedite recovery.

Based on our assessments in the field, it is evident that we must make sure that transit agencies have a comprehensive training program for front-line employees. Working with FTA and a peer advisory group of transit police chiefs and security directors, TSA has produced a training plan to guide transit agencies in providing basic and follow-on training for the range of their employees—train operators, station managers, control system personnel, and various levels of management. To expedite improvement in this area, we have recently amended the Transit Security Grant Program to streamline the application process to ensure quick, priority funding for employee training. We have also provided the option for transit agencies to request reprogramming of their prior grant funding so they may quickly address this deficiency.

As noted, TSA is using the TSGP to drive improvement in the six security fundamental areas, most notably training for key personnel, drills and exercises and public awareness and preparedness. Elevated posture in these areas provides the foundation for an effective transit security program.

The $175 million TSGP is the centerpiece of DHS's interagency strategy to close gaps between operator security status and baseline standards. For purposes of the TSGP, "transit" includes Amtrak, which is eligible for $8.3 million, and commuter ferry systems, which are eligible for $7.8 million. The TSGP guidance emphasized the six fundamental principles previously mentioned, as well as efforts in support of the national preparedness architecture. We are directing transit grant awards based on the results of the system security assessments, the security fundamentals, and support of national preparedness. DHS leverages the grants program to close the gaps at high risk properties.

Highway (Bus and Trucking)-Close Gaps. TSA is working on a number of strategies to close gaps in performance versus actual standards. We are currently considering a number of voluntary incentive programs and regulatory options. TSA, in partnership with G&T, is using the Intercity Bus Security Grants Program which was funded at $12 million in FY 2007 to close gaps in the over-the road bus industry and the Trucking Security Program also funded at $12 million in FY 2007 to address security issues in the trucking industry.

Pipeline-Close Gaps. TSA has had an extensive working relationship with the pipeline industry. TSA has prepared an employee security awareness training program for all pipeline employees, worked with operators to prepare or im-

prove security plans, conducted site specific visits to evaluate security practices, and developed risk mitigation strategies for high risk assets. This cooperative relationship has resulted in improved conformity to baseline standards.

Enhanced Systems of Security

The final part of our strategy is to enhance the systems of security. As we take actions to close gaps, we also need to improve security technology and explore the way these technologies may apply to multiple modes of transportation.

DHS is developing a number of screening techniques and technologies which may be implemented or deployed quickly to systems facing a specific threat, or in support of major events such as National Special Security Events (NSSEs). Pilot programs to test these technologies are already underway in several major American cities.

Through the DHS Science and Technology (S&T) Directorate's Rail Security Pilot (RSP), DHS has field tested the effectiveness of explosives detection techniques and imaging technologies in partnership with the Port Authority of New York and New Jersey. Close coordination between TSA and S&T ensures that technology development and testing for the mass transit environment align with TSA's strategic priorities. To ensure technology enhances security capabilities in transit agencies, the Federal effort seeks development of mobile and fixed systems amenable to the demands of the transit environment that may be deployed flexibly for maximum deterrent effect and protection of high risk infrastructure. Pilot testing will employ equipment in this manner to validate capabilities most effectively. Future research and development initiatives will maintain this focus.

The Systems Support Division (SSD) of G&T has conducted operational tests to evaluate manufacturer claims on ballistic-resistant trash receptacles and published a report of its findings to help ensure mass transit systems, among others, have the facts needed to guide critical procurement decisions. Similarly, SSD has published a closed circuit television (CCTV) technology handbook to provide a reference point on current CCTV technologies, capabilities and limitations.

Finally, we maintain mobile security equipment, which can fit into two standard size shipping containers, for rapid deployment for use in screening and detection at any major system in the country should the need arise.

In addition to technologies that may apply primarily to passenger modes, TSA is working closely with a number of parties to develop advanced railcar tracking systems with geofenced event-notification capabilities. TSA is also cooperating in efforts to develop next generation hazardous materials rail cars designed to better withstand terrorist attacks and operating accidents.

TSA is working with selected hazardous material carriers to test truck tracking and control technologies. We are also in the early stages of security technology applications to the pipeline industry. Two specific areas TSA is involved in are blast mitigation and unmanned aerial surveillance vehicles.

Presidential Action and TSA's Objectively Measured Risk Reduction Process

On December 5, 2006, the President issued Executive Order 13416, which builds upon the improvements made in surface transportation security since September 11, 2001, specifically actions taken under Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection" (HSPD–7). Executive Order 13416 requires the strengthening of our Nation's surface transportation systems by the facilitation and implementation of a comprehensive, coordinated, and efficient security program. As the Federal official with principal responsibility for protecting surface transportation infrastructure, Secretary Chertoff has the lead in implementing this policy in coordination with the Secretary of DOT and the heads of other relevant agencies. The order sets deadlines for key security activities including security assessments of each surface transportation mode and an evaluation of the effectiveness and efficiency of current Federal Government surface transportation security initiatives. We continue to build upon current security initiatives to develop a comprehensive transportation systems sector specific plan, as defined in the National Infrastructure Protection Plan (NIPP). The five-part strategy cited earlier in my testimony is meeting the requirements of the Executive Order.

Annexes to DHS-DOT Memorandum of Understanding

Three annexes to a September, 2004 memorandum of understanding between DHS and DOT have been completed and signed, evidencing the close and continuous cooperation between TSA and DOT to leverage resources.

The first, between TSA and FRA, memorializes how we will coordinate our programs and initiatives at an agency level to better secure passenger and freight railroad transportation, and improve stakeholder relationships, and to include assisting railroads in prioritizing assets and addressing current and emerging threats and vulnerabilities. While TSA is responsible for rail security and FRA is responsible for

rail safety, the annex provides detailed operational guidance to enable the two agencies to avoid duplication and maximize efficiency and cooperation in their planning, inspection, training and enforcement activities.

The second annex is between the Pipeline and Hazardous Materials Safety Administration (PHMSA) and TSA. This annex delineates our respective roles and responsibilities regarding pipelines and hazardous materials transportation security. It discusses sharing data and compliance information between the agencies, coordinating research and regulatory activities, providing joint public information and emergency response materials, collaboration in inspection and enforcement activities, and sharing technical support.

The third annex is between the Federal Transit Administration (FTA), DHS/G&T, and TSA. It similarly provides for close and continuous cooperation between the two respective agencies in matters relating to security of the Nation's transit systems. Eight working groups have been established under the Annex, coordinating Federal efforts in such areas as security training, security standards development, assessments, exercises, public awareness, and information sharing.

Together, these annexes allow much more efficient use of the government's time and money, while maximizing the value of what these agencies can achieve for industry and the traveling public.

Summary

TSA has a clear strategy to address surface transportation security. That strategy focuses first on identifying areas of high risk and then establishing baseline security standards to address those risks. Once baseline standards are established, we assess the actual status of security in the transportation industries, and in close coordination with stakeholders, devise strategies for bringing actual practices up to the standards we have established. Finally, we are developing advanced systems of security through a coordinated research and development program, to further enhance security beyond the baseline standards. In furtherance of this strategy, I have established an Office of Transportation Sector Network Management specifically to address the cross-cutting issues that affect all aspects of the transportation sector as a unified whole. The intermodal members of this Office are implementing our transportation security strategy through cooperation with stakeholders where appropriate, regulation and inspection where necessary, and through the distribution of grants to assist the industry to implement these objectives we have set forth.

I understand that rail and surface transportation security legislation is a priority for the Committee. The Department and TSA look forward to working cooperatively with the Committee as we have in the past.

Regarding the recently proposed legislation, H.R. 1269, we agree with many of the objectives of its provisions. The commitment to a comprehensive program for sustained security enhancement is laudable. As such, there is much opportunity to work together toward our common purpose of bolstering security in transit agencies nationwide. Working with the Committee, we will aim to ensure that deadlines in the bill are realistic, that mandates are not so proscriptive as to constrain executive action and flexibility in the execution of security programs, that funding levels are focused on high—consequence risk reduction, and that new legislative requirements do not merely duplicate our current efforts. We appreciate your initiative in this area, which provides a framework for further discussions as the legislative process moves forward.

Thank you for this opportunity to inform you of our efforts in freight rail, commuter rail and other transit, trucking and pipeline security. I would be happy to answer any questions that you might have.

Mr. THOMPSON. Thank you very much for your testimony.

I now recognize Mr. Rosapep to summarize his statement for 5 minutes.

STATEMENT OF TERRY ROSAPEP, DEPUTY ASSOCIATE ADMINISTRATOR, PROGRAM MANAGEMENT, DEPARTMENT OF TRANSPORTATION

Mr. ROSAPEP. Thank you. Chairman Thompson and Ranking Member King and members of the committee, on behalf of the secretary of transportation and the administrator of the Federal Transit Administration, I am pleased to have this opportunity to update you on FTA's public transportation security program.

America's transit systems are complex, dynamic and inter-connected. Comprised of over 6,000 individual transit operators, these systems by nature are open and accessible and therefore, difficult to secure. Each work day public transportation moves approximately 14 million passengers in the United States.

After 9/11, FTA developed an aggressive transit security initiatives program. Key elements of this program included conducting readiness assessments at 37 of the largest transit systems, representing upwards of 90 percent of all transit riders. These assessments provided a comprehensive view of transit system preparedness, gaps and additional needs and helped shaped the development of three important priorities that continue to form the fundamental baseline of transit security, that being employee training, public awareness and emergency preparedness.

Another key initiative was an outreach effort called connecting communities security and emergency preparedness forums. These forums held at 18 regions across the country improved public agency coordination and planning efforts between transit agencies, emergency management agencies, law enforcement and other partners.

Another activity involved deploying technical assistance teams on-site at the 50 largest transit agencies. The technical assistance teams used FTA's top 20 security action items as an assessment tool to help transit agencies identify any gaps in their security program and develop products to fill those gaps.

Finally, security drill and exercise grants were provided to over 80 transit agencies. These grants helped transit agencies plan, conduct and evaluate various types of security exercises ranging from tabletop programs to large-scale interagency regional drills.

In September of 2005, FTA, the Transportation Security Administration, and the Office of Grants and Training signed an annex to the DOT/DHS memorandum of understanding regarding security roles and responsibility. This MOU annex provides a structured framework for close collaboration among the federal partners.

FTA, TSA and G&T continue to build upon the initial post–9/11 security initiatives in partnership with industry stakeholders such as the American Public Transportation Association and local transit agencies. Key activities now underway include an eyes and ears public awareness toolkit known at transit watch. Transit agencies can use the toolkit material or customize them to fit their own specific need such as the New York City subway systems' see something, say something message to educate passengers to be mindful of their environment and how to react should they see something suspicious.

In the area of training, the curriculum has been expanded with the addition of new security forces such as the terrorist activity recognition and reaction training course for frontline transit employees. Almost 8,000 employees have taken this training. And another course titled strategic counterterrorism for transit managers has been delivered to over 750 transit managers.

Another initiative is the connecting communities forums. The next phase of these new updated forums has begun. Last month a connecting communities forum was held in the national capital region at the WMATA training facility.

Reflecting the importance of stakeholder outreach, FTA, TSA and G&T are conducting semi-annual safety and security roundtables to address direct stakeholder outreach. The roundtables bring together the safety and security chiefs of the 50 largest agencies plus other key industry leaders for peer-to-peer informational exchanges. The last roundtable was held in Newark, New Jersey in December. And the next roundtable is tentatively scheduled for Chicago this spring.

And finally, we are working with our federal partners to develop security standards to provide transit agencies with consistent benchmarks and recommended practices. Leveraging the success of the FTA–APTA process for developing standards in other areas, we are proceeding closely with our federal partners to develop standards in key security areas such as infrastructure protection, risk assessment and emergency preparedness.

Mr. Chairman, members of the committee, please be assured that FTA will continue to work closely with Congress and our partners at DHS to strengthen the nation's public transportation security.

Thank you for this opportunity to speak today. And we will be happy to answer any questions you may have.

[The statement of Mr. Rosapep follows:]

PREPARED STATEMENT OF TERRY ROSAPEP

Chairman Thompson, Ranking Member King, and other members of the Committee, thank you for this opportunity to testify today on behalf of the Secretary of Transportation and the Federal Transit Administration (FTA). I am pleased to have this opportunity to update you on transit security and how the U. S. Department of Transportation's (DOT) initiatives in that area support the Department of Homeland Security's (DHS) transportation security mission. Additional DOT initiatives in support of railroad security were previously detailed in the Federal Railroad Administration's February 6 testimony before this committee, and I refer the Committee to that Statement.

FTA and Transit Security

America's transit systems are dynamic, interconnected, and composed of over 6,000 local systems. Unlike airports, these systems are also inherently open, and therefore difficult to secure. In New York's Penn Station alone, more than 1,600 people per minute pass through its portals during a typical rush hour. The combination of open access and large numbers of people makes transit systems an inviting target for those who seek to cause the United States harm. The deliberate targeting of the public transportation systems in Tokyo, Moscow, Madrid, and London by terrorists underscores this point.

FTA, the Federal Railroad Administration (FRA), other Federal and State partners, and the transit industry have built a solid foundation for security in the years following the attacks of September 11, by focusing on three security priorities: public awareness, employee training, and emergency preparedness. After September 11, 2001, FTA undertook an aggressive nationwide security program and led the initial Federal effort on transit security. The initial response included conducting threat and vulnerability assessments in 37 large transit systems, 30 of which carry almost 90 percent of all transit riders. The assessments at that time gave us a comprehensive view of transit system readiness, vulnerabilities, and consequences, and identified the three important priorities that continue to form the fundamental baseline of DOT's transit security initiatives.

Today, under Executive Order 13416, FTA, in partnership with FRA and DHS, continues to build upon these priorities as they provide focused benefits to the dynamic, open nature of America's transit network. Employee Training develops the skills of 400,000 front-line transit employees, who are the eyes and ears of the transit network, and first line of defense against terrorism. Public Awareness programs such as Transit Watch educate passengers to be mindful of their environment, and how to react should they see something suspicious. Emergency Preparedness programs build local, collaborative relationships within communities that allow for quick and coordinated response in a crisis. Over the last five years, we have learned

that terrorists adapt and change their strategies in response to security measures. But regardless of where an attack comes from or how it is devised, security training of employees and the awareness of passengers can help to prevent or mitigate it.

In 2002, to help guide transit agency priorities, FTA issued a "Top 20 Security Action Item List" to improve transit safety and security operations, particularly with regard to employee training, public awareness, and emergency preparedness. In a joint effort coordinated with the Mass Transit Sector Coordinating Council, FTA, and the Transportation Security Administration (TSA), the Security Action Items for transit agencies were revised in 2006.

The Safe, Accountable, Flexible, Efficient Transportation Equity Act—A Legacy for Users (SAFETEA–LU) mandates several steps to move transit security forward through collaboration among Federal, State, local, and private entities. In September 2005, FTA and two agencies within DHS—TSA and the Office for Domestic Preparedness, now the Office of Grants and Training (G&T)—signed the Public Transportation Security Annex to the DOT/DHS Memorandum of Understanding (MOU) on security. The MOU recognizes that DHS has primary responsibility for transportation security and that DOT plays a supporting role, providing technical assistance and assisting DHS when possible with implementation of its security policies as allowed by DOT statutory authority and available resources. The Annex identifies specific areas of coordination among the parties, including citizen awareness, training, exercises, risk assessments, and information sharing. To implement the Annex, the three agencies have developed a framework that leverages each agency's resources and capabilities.

With the Annex in place as a blueprint, FTA, TSA and G&T have established an Executive Steering Committee. Since 2005, the Executive Steering Committee has interacted with DHS, DOT, FRA and transit industry leaders. This committee oversees eight project management teams that spearhead the Annex's programs. Each of these programs advances one or more of FTA's three security priority areas (public awareness, employee training, and emergency preparedness). We have been implementing the Annex energetically since its inception.

The eight teams are as follows:

1. *Risk Assessment and Technical Assistance Team*

The Risk Assessment and Technical Assistance team is using a risk-based approach to transit security, working toward one industry model for conducting transit risk assessments. The team issued the "TSA/FTA Security and Emergency Management Action Items" and is developing the Next Generation Security and Emergency Management Technical Assistance Program Master Plan to identify and prioritize industry security needs.

2. *Transit Watch and Connecting Communities Team*

The Transit Watch and Connecting Communities team is reinstating and expanding these two FTA programs, which foster public awareness and coordinated emergency response. The initial roll-out of Transit Watch helped to institute this program at many transit agencies across the country. The next phase of Transit Watch, recently released, includes a focus on unattended bags, Spanish language materials and emergency evacuation instructions. Twelve new Connecting Communities forums are scheduled for 2007; the second forum is being held this week in the National Capitol Region, at WMATA's Turner facility in New Carrollton, Maryland.

3. *Training Team*

The Training team is developing new courses on timely security topics such as security design considerations and National Incident Management System (NIMS) for transit employees, and also working towards developing one integrated security training curriculum.

4. *Safety and Security Roundtables TeamThe Safety and Security Roundtables team works on direct stakeholder outreach. They are responsible for planning two roundtables each year for the safety and security chiefs of the 50 largest transit agencies and Amtrak. The roundtable format emphasizes peer-to-peer informational exchanges among the participants. The last roundtable was held in Newark, New Jersey in December 2006 and the next roundtable is tentatively scheduled for Chicago this spring.*

5. *Web-based National Resource Center Team*

The Web-based National Resource Center team is developing a secure library site for information on best practices, grants, and other security matters. Access to the National Resource Center will be available to security chiefs of transit agencies.

6. *Emergency Drills and Exercises TeamThe Emergency Drills and Exercises team is updating the program to incorporate DHS Exercise program guidance. The scope of this effort includes both tabletop exercises and regional field drills.*

7. *Annual Plan and Grant Guidance Team*

FTA lends its subject matter expertise to the DHS Infrastructure Protection grant process. In the context of the MOU Annex, FTA is also able to leverage its long-standing working relationships with transit agencies to help TSA vet security initiatives.

8. *Standards and Research TeamThe Standards and Research team's primary focus is the development of industry security standards. This is a critical area because it provides transit agencies with consistent industry benchmarks and recommended practices. Leveraging the success of the FTA, FRA and American Public Transportation Association (APTA) process for developing standards in other areas, FTA is proceeding closely with its Federal partners to develop standards in key areas such as infrastructure protection, risk assessments and emergency preparedness.*

I would like to add that FTA also supports security projects through its Urbanized Area Formula Grant Program. Under this program, transit agencies are required to spend at least 1 percent of their annual formula fund allocation on public transportation security, or to certify that they do not need to spend 1 percent of their allocation for such purposes. For transit agencies in Urbanized Zone Areas (UZAs) over 200,000 in population, only capital projects are eligible to count towards the 1 percent security threshold. SAFETEA-LU usefully expanded the definition of capital projects to include security planning, training and emergency drills and exercises. In contrast to TSA's broad statutory authority for security in all modes of transportation, FTA has limited statutory and regulatory authority on security matters, and does not have a dedicated security grant program. FTA has done a great deal to assist transit agencies in improving their security practices through training programs, research, technical assistance and oversight activities. FTA and FRA continue to work together to improve passenger rail and rail transit security. FTA will continue to use all of these resources, in close collaboration with TSA and G&T to improve transit security.

I want to assure you that FTA has been, and is, using all of the resources and capabilities in its toolbox to strengthen the joint security initiative formalized in the September 2005 Public Transportation Security Annex to the DOT/DHS MOU. The MOU Annex expands that toolbox. Since September 11, 2001, transit security has benefited from exceptionally strong partnerships, and genuinely collaborative initiatives, among the industry, different agencies and departments, and the MOU Annex captures that spirit of cooperation.

Please also be assured that the FTA will continue to strengthen public transportation security. We look forward to continuing to work with Congress to achieve the goal of protecting our Nation's public transportation infrastructure. I would be happy to answer any questions you may have. Thank you.

Mr. THOMPSON. Thank you very much for your testimony.

I now recognize Mr. Fairfax to summarize his statement for 5 minutes.

STATEMENT OF RICHARD FAIRFAX, DIRECTOR OF ENFORCEMENT PROGRAMS, OCCUPATIONAL SAFETY AND HEALTH ADMINISTRATION, DEPARTMENT OF LABOR

Mr. FAIRFAX. Good morning, Chairman Thompson and ranking member, distinguished members of the committee. Thank you for the opportunity to appear before you today to discuss OSHA's administration of the whistle-blower provision for the 14 statutes that we enforce.

While the administration has not taken an official position on the whistle-blower legislation you are considering, I will be able to discuss the scope in OSHA's administration of these statutes and how OSHA addresses the respective whistle-blower complaints, which we hope will be of assistance to you.

When the Occupational Safety Act law was passed in 1978, OSHA authority was limited to a single statute, section 11C of the OS Act. Currently we employ approximately 72 field investigators that enforce 14 whistle-blower statutes. Also under OSHA, 26

states operate their own state plan programs under section 18 of the OS Act. And under this section, they enforce their equivalent of section 11C of the OS Act. For the other 13 statutes, OSHA enforces those in those state planned states.

The general provisions of each statute are administratively enforced by the primary agency while OSHA administers only the whistle-blower provisions of those statutes. A whistle-blower complaint under any of the 14 statutes is based on the belief by an employee that he or she has been retaliated against through an unfavorable personnel action for that employee's engagement in a protected activity. In some cases, complainants can file under more than one statute.

To establish a violation under any of the 14 statutes, our investigators have to establish a prima facie case which consists of four elements.

The first is that protected activity, meaning the OSHA, must establish that the complainant engaged in an activity protected by this specific statute.

Employer knowledge: OSHA must establish that the person involved in the decision to take adverse action was aware of or suspected that the complainant engaged in a protected activity.

Adverse action: OSHA must establish the complainant suffered from some form of adverse employment action initiated by the employer.

And finally, nexus: OSHA must establish a causible link or a nexus between the protected activity and the adverse employment action.

In investigating a whistle-blower complaint under any of the statutes, the Department of Labor does not represent the complainant nor the respondent, but, in fact, is a neutral fact finder. Investigators must test both the complainant's allegation and the respondent's non-retaliatory reason for the alleged adverse action.

Consequently, investigations can become quite complicated and time consuming as multiple interviews are required and evidence along with it—multiple interviews are required and gathering evidence along with statements must be verified. If the investigator is unable to prove by the preponderance of evidence that any of the elements form a prima facie case, we dismiss the complaint.

An investigation consists of gathering evidence by two principle means, both interviewing the complainant and all the respondent's witnesses and the complainant's witnesses and then collecting documentary evidence. Once the investigative report is written, the secretary's findings can be issued. The statutes require that the secretary through OSHA either dismiss the case or find reasonable grounds to believe that a violation of the relevant statute has occurred.

We call this in our lingo a merit case. In a merit case, the remedies available and permitted vary according to the individual statute. Remedies not only involve corrective action for the complainant, but also involve issues to address the impact of the violation in the workplace. Both complainants and respondents have the right to appeal 11 of the 14 statutes. These appeals go before an administrative law judge. And then both parties can further appeal this before the administrative review board.

I would like to take a few moments and just, I guess, talk about the program. Presently we average about 1,900 cases a year under our 14 statutes. Remember that we only have 72 investigators. While the statutes have differing prescribed timeframes for completion of the investigation and issuance of findings, we have found that we are seldom able to meet our time requirements to complete these investigations.

Despite the increased number of the statutes and increasing number of complaints filed under the newer statute, the total number of complaints varies each year from 1,800 to 2,100. The outcomes of the complaints for the fiscal year 2006 are consistent with past years. Of the approximately 1,900 complaints we investigated, 65 percent we dismissed.

Fourteen percent were withdrawn by the complainant, and approximately 22 percent we found in favor of the complainant. Of that 22 percent, 66 were settled by OSHA. Twenty-eight percent were settled by the parties themselves. And approximately 6 percent were not settled, and we issued a merit finding.

In conclusion, I hope the testimony has shed light on our complex process by which we cover whistle-blower complaints under the 14 statutes.

And I would be more than happy to answer any questions the committee may have. Thank you.

[The statement of Mr. Fairfax follows:]

PREPARED STATEMENT OF RICHARD E. FAIRFAX

Good morning Chairman Thompson, Ranking Member King, distinguished Members of the Committee, ladies and gentlemen. Thank you for the opportunity to appear before you today to speak to you about OSHA's administration of the whistleblower provisions of fourteen statutes. Also, I understand the Committee would like the Department’s views on the "Rail and Public Transportation Security Act of 2007." The Administration does not yet have an official position on the legislation so I will not be able to comment on specific provisions in the bill. As a general matter, however, we would caution that an overly broad expansion of covered protected activity, particularly combined with a broad definition of adverse action, could result in the Department of Labor becoming the arbiter of another agency's employment disputes, which could also be resource-intensive for the Department.

Organization and Responsibilities

When the Occupational Safety and Health Act became law in 1970, OSHA had no specific program for investigating complaints filed under the Act’s whistleblower provision, Section 11(c). Initially, complaints were investigated by Compliance Safety and Health Officers in the field. By 1974, it had become apparent that specialized skills were needed to conduct retaliation investigations, and in 1975, a central whistleblower investigation office was established. This office consisted of two supervisors and ten investigators, all located in the ten regional offices around the country. By 1980, there were over 70 investigators and supervisors. In 1981, the whistleblower program was again decentralized, with responsibility delegated to each of the ten Regional Administrators. Currently, the whistleblower program employs 72 full-time field investigators, nine supervisors, and one program manager in the field.

Under my direction, the Office of Investigative Assistance (OIA) develops policies and procedures for the Whistleblower Protection Program, administers appeals of cases dismissed under 11(c), the Asbestos Hazard Emergency Response Act of 1986 (AHERA), and the International Safe Container Act (ISCA), develops and presents formal training for Federal and State field staff, and provides technical assistance and legal interpretations to field investigative staff. OIA employs six staff.

Twenty-six states operate state plans pursuant to Section 18 of the Occupational Safety and Health Act of 1970, which provides that any state that desires to assume responsibility for development and enforcement of occupational safety and health standards may do so. To establish a state plan, a state must submit to the Secretary of Labor a state plan for the development of such standards and their enforcement.

Private-sector employees in state plan states may file occupational safety and health retaliation complaints with either federal OSHA or the state or both. Complaints under any of the other thirteen whistleblower statutes administered by OSHA fall under the jurisdiction of Federal OSHA.

History of Delegation of Statutes to OSHA

In the 1980s and 1990s, because of the perceived expertise of the OSHA retaliation investigators, whistleblower investigative and administrative responsibilities under the Surface Transportation Assistance Act of 1982 (STAA), ISCA, and AHERA were delegated to OSHA to administer. For similar reasons, in 1997, under an agreement with the Department’s Wage & Hour Division, the enforcement of the whistleblower provisions of six environmental statutes and the nuclear safety statute, the Energy Reorganization Act (ERA), was delegated to OSHA.

In 2001, the enforcement of the whistleblower provisions of the Wendell H. Ford Aviation Investment and Reform Act for the 21st Century (AIR21) was added, and in 2002, the enforcement of the whistleblower provisions of the Sarbanes-Oxley Act, (SOX) and the Pipeline Safety Improvement Act of 2002 (PSIA) was also added.

The Fourteen Whistleblower Statutes Administered by OSHA

The whistleblower provisions of the following statutes are administered and enforced by the primary agency. For example, OSHA enforcement officers investigate the safety or health complaints underlying a whistleblower complaint, the FAA investigates airline safety complaints, the Federal Motor Carrier Safety Administration investigates violations of commercial motor carrier safety complaints, and the SEC investigates allegations of corporate fraud.

- Section 11(c) of the Occupational Safety and Health Act of 1970 (11(c))
- Asbestos Hazard Emergency Response Act of 1986 (AHERA)
- Clean Air Act of 1977 (CAA)
- Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (CERCLA)
- Energy Reorganization Act of 1978 (ERA)
- Federal Water Pollution Control Act of 1972 (aka Clean Water Act) (FWPCA)
- International Safe Container Act of 1977 (ISCA)
- Pipeline Safety Improvement Act of 2002 (PSIA)
- Surface Transportation Assistance Act of 1982 (STAA)
- Safe Drinking Water Act of 1974 (SDWA)
- Solid Waste Disposal Act of 1976 (SWDA)
- Corporate and Criminal Fraud Accountability Act of 2002, Title VIII of the Sarbanes-Oxley Act of 2002 (SOX)
- Toxic Substances Control Act of 1976 (TSCA)
- Wendell H. Ford Aviation Investment and Reform Act for the 21st Century (AIR21)

Jurisdiction

Investigators must confirm that complaints fall within the jurisdiction of a whistleblower statute administered by OSHA. Investigators review every new case upon assignment to ensure the complaint was timely filed, that a prima facie allegation is present under one of the statutes, and that the case has been properly docketed and all parties notified. If he or she has not already done so, the investigator checks on prior or current retaliation, safety and health, or other regulatory cases related to either the complainant or the employer. This enables the investigator to coordinate related investigations and obtain additional background data pertinent to the case at hand. If the complaint fails to meet any of the elements of a prima facie allegation, or if other jurisdictional issues preclude the continuation of the investigation, the complaint must be dismissed, unless it is withdrawn.

The Elements of a Violation

Under the whistleblower statutes, employers are not permitted to retaliate against an employee for engaging in activities protected by statute. To prove a violation, each of the four elements of a *prima facie* allegation must be proven. The elements are:

Protected Activity

It must be established that the complainant engaged in activity protected by the specific statute(s) under which the complaint was filed. Protected activity generally falls into four broad categories: providing information relating to an alleged violation of the law to a government agency (e.g., OSHA, FMCSA, EPA, NRC, DOE, FAA, SEC, DOT), a supervisor (the employer), a union, health department, fire department, Congress, or the President; filing a complaint or instituting a proceeding provided for by law, for example, a formal occupational safety and health complaint to OSHA under Section 8(f); testifying in proceedings; and, under some of the stat-

utes, refusing to perform an assigned task on the basis of a reasonable apprehension of death or serious injury or refusing to perform a task that is deemed illegal under the specific statute(s).

Employer Knowledge

The investigation must show that a person involved in the decision to take the adverse action was aware, or suspected, that the complainant engaged in protected activity. For example, a respondent manager need not have specific knowledge that the complainant contacted a regulatory agency if the complainant’s previous internal complaints would cause the respondent to suspect a regulatory action was initiated by the complainant.

Adverse Action

The evidence must demonstrate that the complainant suffered some form of *adverse employment action* initiated by the employer. Although the language of the statutes may differ, they frequently use the terms "discharge or otherwise discriminate." The phrase adverse employment action has been defined in the decisions of many courts, including the Supreme Court. This is an area of the law that is currently in flux, and investigators and supervisors regularly review decisions to keep up-to-date on case law. Examples of retaliatory employment actions include discharge, demotion, reprimand, harassment, lay-off, failure to hire or recall, failure to promote, blacklisting, transfer to a different job, change in duties or responsibilities, denial of overtime, reduction in pay, denial of benefits, and constructive discharge, wherein the employer *deliberately* created working conditions that were so difficult or unpleasant that a reasonable person in the employee's situation would have felt compelled to resign.

Nexus

A causal link—nexus—between the protected activity and the adverse action must be established. Nexus cannot always be demonstrated by direct evidence, such as animus (exhibited animosity) toward the protected activity. It may also involve proximity in time between the protected activity and the adverse action (timing), disparate treatment of the complainant in comparison to other similarly situated employees, false testimony or manufactured evidence, or a pretextual defense put forth by the respondent.

Under ten of the statutes administered by OSHA, a complainant must prove by a preponderance of the evidence that the alleged adverse action was motivated by the alleged protected activity in order to establish that the law was violated. Under four of the statutes, a complainant must prove by a preponderance of the evidence that the alleged protected activity was a contributing factor to the alleged adverse action. Once a complainant establishes a prima facie case that his or her protected activity was either a motivating or contributing factor in the adverse action, the burden of production shifts to the respondent to articulate a reason for the adverse action. The burden then shifts back to the complainant to establish that the respondent's articulated reason was a pretext for discrimination or that the respondent's reason, while true, is only one of the reasons for its conduct, and that another reason was complainant’s protected activity. To avoid liability in a "mixed motive" case, the respondent must demonstrate, depending on the statute, either by a preponderance of the evidence or by clear and convincing evidence, that it would have taken the same adverse action notwithstanding the complainant's protected activity.

Investigating Complaints

DOL does not represent either the complainant or the respondent; as neutral fact-finders, investigators must test both the complainant’s allegation and the respondent’s non-retaliatory reason for the alleged adverse action. It is on this basis that relevant and sufficient evidence is identified and collected in order to reach the appropriate disposition of the case. If the complainant is unable to prove by preponderance of the evidence any of the elements of a *prima facie* allegation, the case is dismissed.

Early Resolution

OSHA makes every effort to accommodate early resolution of complaints in which both parties seek resolution prior to the completion of the investigation. An early resolution is often beneficial to both parties, since potential losses are at their minimum when the complaint is first filed. Consequently, the investigator is encouraged to contact the respondent immediately after completing the evaluation interview if he or she believes an early resolution may be possible. However, the investigator must first determine if an inspection or investigation under the substantive provisions of the various statutes is planned prior to any contact with a respondent, so as not to inadvertently give notice to the respondent of an imminent OSHA (or FAA

or other) inspection. Thereafter, at any point the investigator can explore how an appropriate settlement may be negotiated and the case concluded.

On-site Investigation

Personal interviews and collection of documentary evidence are conducted on-site whenever practicable. Generally, investigators personally interview all appropriate witnesses during a single site visit. The respondent's designated representative has the right to be present for all management interviews, but interviews of employees are to be conducted in private. In limited circumstances, testimony and evidence may be obtained by telephone, mail, or electronically.

Interviewing the Complainant

The investigator generally arranges to meet with the complainant as soon as possible to interview and obtain a statement detailing the complainant's allegations.

The complainant is asked to provide a list of witnesses and all documentation in his or her possession relevant to the case. The investigator also ascertains the restitution sought by the complainant and advises the complainant of his or her obligation to seek employment, in order to mitigate any possible damages, and to maintain records of interim earnings.

Contact with the Respondent

Following receipt of OSHA's letter notifying the respondent of the complaint, the respondent submits a written position statement, which may or may not include supporting evidence. In some instances, the material submitted may be sufficient to adequately document the company’s official position. However, in most cases, the investigator needs to visit the respondent's worksite to interview witnesses, review records and obtain documentary evidence, or to further test the respondent's stated defense.

The investigator generally interviews all company officials who had direct involvement in the alleged protected activity or retaliation, and attempts to identify other persons (witnesses) at the employer's facility who may have knowledge of the situation. While at the respondent's establishment, the investigator makes every effort to obtain copies of, or at least review and document in a memorandum to file, all pertinent data and documentary evidence which the respondent offers and which the investigator determines is relevant to the case.

If necessary, subpoenas may be obtained for testimony or records when conducting an investigation under § 11(c) or AHERA. The other whistleblower provisions do not authorize subpoenas. If the respondent fails to cooperate or refuses to respond, the investigator evaluates the case as best as possible and makes a determination based on the available evidence.

Analysis

After having gathered all relevant evidence available and resolved any discrepancies in testimony, the investigator evaluates the evidence and draws conclusions based on the evidence and the law, according to the requirements of the statute(s) under which the complaint was filed.

Upon completion of the field investigation and after discussion of a non-meritorious case with the supervisor, the investigator again contacts the complainant in order to provide him or her the opportunity to present any additional evidence the complainant deems to be relevant. If the complainant offers any new evidence or witnesses, the investigator then ascertains whether such information is relevant, and if so, what further investigation might be necessary prior to final closing of the case.

Documenting the Investigation

Investigators document any and all activities associated with the investigation of a case, developing a substantial case file that contains the original complaint; the respondent's response(s); all of the documentary evidence; memoranda to the file about every contact with any party or witness that is otherwise not documented, such as through a witness statement; all correspondence to or from the parties, other government agencies, or others; results of any research conducted; the Final Investigative Report; and a copy of the Secretary's Findings or other correspondence closing the case.

Issuance of Secretary's Findings and Orders, if Appropriate

Once the Final Investigative Report is written, the investigator forwards it, together with the case file, to the supervisor for review and concurrence, so that Secretary's Findings can be issued. This allows either dismissal of the case or a finding of a violation of the relevant statute. If there is a violation, the investigator, where appropriate, broaches the subject of settlement with the respondent. If the respondent is amenable, settlement negotiations may be initiated. The appropriate remedy

in each individual case will already have been carefully explored and documented by the investigator.

Remedies

The remedies available and permitted vary according to statute, and are subject to legal interpretations and decisions. Remedies not only involve corrective actions for the individual who filed the complaint, but also address the impact of the violation on the entire work force. Thus, to prevent a chilling effect or to ensure that a similar violation does not recur, orders may include requirements for posting, management training, and informational speeches to workers and their representatives.

Full relief of the complainant’s loss is generally sought during settlement negotiations, but compromises may be considered in appropriate cases to accomplish a mutually acceptable and voluntary resolution of the matter. If settlement is reached, an agreement is signed and the case is closed. If an equitable settlement is impossible, OSHA issues to the respondent Secretary’s Findings and an Order, by way of which the complainant is made whole. Restitution may encompass any or all of the following, and it is not necessarily limited to these:

•7 Reinstatement or preliminary reinstatement—depending on the statute under which the complaint was filed—to the same or equivalent job, including restoration of seniority and benefits that the complainant would have earned but for the retaliation.

• Wages lost due to the adverse action, offset by interim earnings.

• "Front pay," which encompasses future wage losses, calculated from the end-date of back-wages, and projected to an agreed-upon future date in cases where reinstatement is not feasible.

• Expungement of all warnings, reprimands, or derogatory references resulting from the protected activity that have been placed in the complainant's personnel file or other records.

• Respondent's agreement to provide a neutral reference to potential employers of the complainant.

• Posting of a notice to employees stating that the respondent agreed to comply with the relevant whistleblower statute and that the complainant has been awarded appropriate relief.

• Compensatory damages, such as out-of-pocket medical expenses resulting from cancellation of a company insurance policy, expenses incurred in searching for another job, vested fund or profit-sharing losses, or property loss resulting from missed payments.

• Compensatory damages under certain statutes, such as for pain and suffering, including mental anguish, the loss of a home, loss of reputation, etc.

• A lump-sum payment to be made at the time of the signing of the settlement agreement as agreed by the parties.

• Punitive damages, under certain statutes, when a management official involved in the adverse action knew about the relevant whistleblower statute before the adverse action or when the respondent’s conduct is egregious.

The Surface Transportation Assistance Act of 1982, the Wendell H. Ford Aviation Investment and Reform Act for the 21st Century (AIR21), the Sarbanes-Oxley Act of 2002 (SOX), and the Pipeline Safety Improvement Act of 2002 (PSIA) authorize the Secretary to order preliminary reinstatement based on her investigative findings. However, in the last few years, the Secretary and complainants have experienced some difficulty in compelling recalcitrant employers to comply with preliminary reinstatement orders issued by either OSHA or the Office of Administrative Law Judges under AIR21 and SOX. Although AIR21 (as well as SOX, by incorporating AIR21) expressly provides that the filing of objections does not stay the Secretary's preliminary order reinstating the employee, the jurisdictional provisions of the statute reference only a section entitled "final orders." Accordingly, a number of judges have held that they lack authority under the statute to enforce preliminary reinstatement orders even though the statute explicitly states that those orders are not to be stayed during the administrative adjudication. Those judges have interpreted the statute as providing the Secretary and whistleblowers with a cause of action to enforce only final orders of the Secretary.

Hearings and Appeals

Because of OSHA's role as a neutral fact-finder, many of its findings are not challenged. Complainants or Respondents who object to OSHA's findings under the Energy Reorganization Act of 1978, the Wendell H. Ford Aviation Investment and Reform Act for the 21st Century, the Sarbanes-Oxley Act of 2002, the Pipeline Safety Improvement Act of 2002, the Surface Transportation Assistance Act of 1982, and the environmental statutes may request a *de novo* hearing before a Department of

Labor Administrative Law Judge (ALJ). After a decision is issued by an ALJ, review of the case is by the Administrative Review Board (ARB), which is authorized to issue final orders of the Secretary of Labor. Depending on the whistleblower law involved, the ARB either reviews the entire ALJ decision under a *de novo* standard of review, or *de novo* on matters of law, and a "substantial evidence" standard of review on the ALJ's findings of fact. Judicial review of final agency decisions is in the U.S. Courts of Appeals.

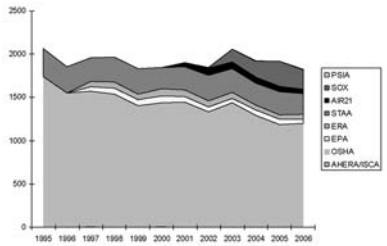
Actions under OSHA, AHERA, and ISCA are enforced by the Secretary in district court. There is no statutory right to appeal OSHA, AHERA, and ISCA determinations by OSHA. The agency-level decision is the final decision of the Secretary of Labor. However, if a complaint is dismissed, the complainant may request from the Director of the Directorate of Enforcement Programs (DEP) a review of the case file. This review is not *de novo.* Rather, a committee constituted of staff of the Office of Investigative Assistance and the Office of the Solicitor's Occupational Safety and Health Division (the appeals Committee) reviews the case file and findings for proper application of the law and for substantial evidence. If the investigation is found to be lacking, the case is remanded to the field to be reopened for further investigation.

Program Performance

The complexity of complaints filed under the more recently enacted statutes has resulted in longer OSHA investigations that exceed in length their statutory timeframes.

Statute	Time-frame	Average Days to Complete	Total Cases
EPAs	30 days	102	57
STAA	60 days	85	246
AIR21		121	54
SOX		150	250
PSIA		84	7
OSHA	90 days	89	1233
AHERA		211	1
Total			1901

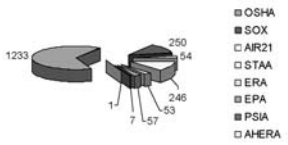
Average Days to Complete Compared to Statutory Timeframes



Cases Received from Fiscal Year 1995 through 2006

Fiscal Year 2006 Performance

OSHA received 1,825 cases in fiscal year 2006. The chart below represents cases completed in fiscal year 2006, broken out by statute.



Complaints Completed in Fiscal Year 2006

This discrepancy between the timeframes prescribed in the statutes and agency practice is not limited to the investigative stage. The Office of administrative Law Judges and the Administrative Review Board face the same challenges. Indeed, two years ago, when Congress amended the Energy Reorganization Act of 1978 (ERA), it added, among other things, the "kick-out" provision allowing complainants to remove a case to U.S. District Court if the Department of Labor failed to issue a final decision within a year, so long as the delay is not due to the bad faith of the complainant. Although the ERA amendments in 2005 did not change the statutory 90-day timeframe for issuing final decisions, we believe that in setting a one-year timeframe for removal to district court, Congress recognized that it is not unreasonable for the Department to take up to one year to complete the investigatory and adjudicative processing of a whistleblower complaint under the ERA.

Despite the increased numbers of statutes and increasing numbers of complaints filed under the newer statutes, the total number of complaints filed annually remains relatively steady at 1,800 to 2,100 complaints per year. However, the proportion of the more complex cases has grown in relation to the simpler cases under the other statutes (see graph below).

The outcomes of OSHA's investigations for fiscal year 2006 are consistent with those of the past five or more years. The results do not vary more than five percentage points from year to years. Twenty-two percent of the investigations resulted in a disposition favorable to the complainant ("merit" cases). Of thes, 66% were settled by OSHA, 28% were settled by the parties themselves, and inthe remainder—7%—OSHA issued findings or preliminary orders in favor of complainants. In addition, 65% were dismissed, and 14% were withdrawn. Generally, investigations leading to dismissal of claims entail as much work and last as long as those leading to findings of violations. OSHA does not track the length of investigations broken out by length of investigation.

The State Plan States had similar results with their 11(c)-type complaints in fiscal year 2006—60% were dismissed; 20% withdrawn; and 20% wre meritorious, of which 75% were settled.

Conclusion

I hope that my testimony has shed some light on the complex process by which whistleblower complaints are resolved. Not only do our investigators juggle the competing demands of numerous open cases at any one time, they must have knowledge and expertise in applying numerous related statutes and implementing regulations

(beyond the 14 whistleblower statutes and their particular implementing regulations). Investigators must know the parlance of, for example, federal criminal fraud statutes, federal securities laws and regulations, Federal Aviation Administration regulations, other Department of Transportation regulations, Nuclear Regulatory Commission regulations and many others.

I look forward to answering any questions you might have.

Mr. THOMPSON. Thank you very much for your testimony.

We now recognize Mr. Falkenrath to summarize his statement for 5 minutes.

STATEMENT OF RICHARD FALKENRATH, DEPUTY COMMISSIONER FOR COUNTERTERRORISM, NEW YORK CITY POLICY DEPARTMENT, CITY OF NEW YORK

Mr. FALKENRATH. Mr. Chairman and Mr. King, thank you very much for the opportunity to appear here this morning. It is a great privilege.

I commend your committee for taking this issue up so early in the 100th Congress. I agree with your assessment of its importance and of the threat to the mass transit systems of this country that you expressed in your opening statement.

I personally wake up every day thinking there could be an attack in New York City. And as I go to work, I think what it could be. I think the single most likely target of a terrorist attack, if I had to pick one, would be an attack on our mass transit systems and in particular, our subway because of the vulnerability of that system, the density of that system, and the demonstrated proclivity of terrorist organizations around the world to attack similar systems in other cities.

I believe that New Yorkers feel the terrorist threat to mass transit more acutely than most other Americans because the city is more intensely reliant on mass transit than any other city in America. New York has the busiest, the densest, the most complex mass transit system in the Western hemisphere.

In your opening statement, you noted that 11.2 million Americans ride mass transit every day. 6.6 million of those are in New York City alone, more than half. The single largest mass transit system is, of course, the New York City subway with 5 million people per day, 5.08 million in September 2006.

And then there are another six rail lines that operate making the rail system immensely complicated. Those rail lines have about 1.5 million in addition. Then we have a bus system that 2.4 million New Yorkers ride every day often connecting to the rail system and a ferry system with over 100,000 people riding the ferry system.

So we have an extraordinarily dense mass transit system. Fewer New Yorkers get to work by car relatively than any other city in America. They ride the mass transit system. So we feel this threat very acutely.

Many different agencies are involved in protecting this system. But the ones who directly protect it are all state and local agencies. There really is no federal presence in the mass transit system itself. This is done at the local level. And I think it is very important for this committee to remember that as you conduct oversight in this area and write legislation, you will often be hearing from federal officials. But always remember that the security is provided

at the local level. And that is why we are grateful for this opportunity to be here today.

The NYPD and our partner agencies have pioneered many innovative counterterrorism tactics for use in the mass transit system. I enumerate them in my written statement. And we think we are doing a reasonably good job.

The commitment of resources to this sector is enormous. We alone, the NYPD, has signed 2,800 police officers just to the subway every single morning. And others are assigned as directed by the police commissioner as needed. And we work very closely with our partner agencies.

Now, I would like to recommend a couple of changes in the draft bill that I reviewed. First, I would note that the federal government is not deficient in any regulatory power relating to mass transit authority. The conferral of regulatory authority in the Aviation and Transportation Security Act, which is now vested in the secretary of homeland security, is extraordinarily broad.

Not to put too fine a point on it, the secretary of homeland security can order just about anything he wishes on an emergency basis and have the force of law behind it. So there is really no shortage of federal regulatory power in this area already.

The reporting requirements in the bill, I respectfully would submit, are excessive. And in particular, we would object to those in section five, which create a large number of reporting requirements that the secretary of homeland security would impose upon state and local and special district agencies to fulfill. I now in New York am involved in reviewing many reports being generated pursuant to federal requirements. I am aware of almost a dozen.

And I have got to tell you, I am going to be very honest here. Very few people take these reports seriously. They are really not that useful for the policy decision makers or the operational decision makers. And the only ones who read them, I think, are the contractors paid to read them and make sure that they are complying with the federal requirement. So, please, pare back section five.

On the grants, three comments also expressed in my written statement. First, I believe the grants should be able to be used for personnel costs, for daily operating security costs. Second, the types of agencies needs to be widened who are eligible to apply for the grants. It is not just transit authorities who are involved in this. It is also law enforcement agencies not directly connected to transit authorities.

And third and finally, I would request that the law direct the secretary of homeland security to distribute all of these funds on the basis of risk. I think that is a very important principle that the Congress really ought to throw its full weight behind. We have not seen that to date out of either the Congress or the executive branch. And we in New York believe we should see that.

Thank you, sir.

[The statement of Mr. Falkenrath follows:]

PREPARED STATEMENT OF RICHARD A. FALKENRATH

Good morning, Mister Chairman, Congressman King, and Members of the Committee. I am honored to have this opportunity to represent the New York City Police Department this morning before your Committee.

For the record, my name is Richard A. Falkenrath,. I am the Deputy Commissioner for Counterterrorism in the New York City Police Department. Prior to joining the NYPD, I was the Stephen and Barbara Friedman at Brookings Institution. From 2001 until 2004, I served on the White staff, first as Director for Proliferation Strategy on the National Security Council staff; then as Special Assistant to the President and Senior Director for Policy and Plans staff within the Office of Homeland Security; and finally, as Deputy Assistant to President and Deputy Homeland Security Advisor. Before government service, I was an Assistant Professor of Public Policy at the John F. Kennedy School of Government, Harvard University.

I commend the Committee for addressing the critical subject of mass transit security so early in the 110th Congress. This subject is one of the foremost counterterrorism concerns of the New York City Police Department.

At your request, I am pleased to provide my views on your Committee's draft "Rail and Public Transportation Security Act of 2007." In certain respects, this testimony builds upon the testimony I provided to the Senate Committee on Homeland Security and government Affairs on September 12, 2006.

New York City's Rail and Public Transportation Systems

New York City has the largest, busiest, most complex rail and mass transit system, in the Western Hemisphere. No U.S. city is as intensely reliant on mass transit as is New York City. For this reason among others, the threat to mass transit in New York is real and New Yorkers feel the terrorist threat to mass transit systems powerfully than most Americans.

There are seven separate passenger rail systems in the New York area:

Transit System	Daily Ridership
Staten Island Rapid Transit	12,800
Amtrak	60,000
Metro-North Railroad	125,000
Port Authority Trans-Hudson (PATH)	230,000
Long Island Rail Road	282,000
New Jersey Transit	857,000
NYC Subway	5,000,000
Total	**6,566,800**

The New York City subway the largest mass transit system in the nation by far, with 840 miles of track and 468 stations. Indeed, New York City has only 35 fewer stations than all of the other subway stations in the country combined. The average weekday subway rider count was 5.08 million in September 2006. By ,contrast, average daily load on U.S. passenger aircraft is approximately two—nationwide.

New York City's transit systems rely on a complex network of underground tunnels, including 22 underwater rail tunnels (three under the Hudson River and 19 under the East and Harlem Rivers), in addition to the two vehicular tunnels under the Hudson, one under the East River and one under New York Harbor. Many of these tunnels are old; several are less structurally robust than we would like.

There are 468 subway stations in New York City; most were built before 1930, only half of which have been renovated over the last twenty years. Four of the busiest are:

Station	Daily Passenger Load
Grand Central Terminal	737,097
Penn Station	594,000
Times Square Subway Station	585,315
Union Square Subway Station	304,292

Two major mass transit hubs are also being constructed in Lower Manhattan at the Fulton Street Station and under the reconstructed World Trade Center.

Each day, an estimated 2.4 million people ride New York City buses, which operate 207 routes daily covering 12,581 bus stops. Tens of thousands of passengers from New Jersey Transit buses, Metropolitan Suburban Bus Authority other systems serving outlying areas make their way into the City and then transfer to MTA buses or the subway.

Finally, an estimated 70,000 people, spread over 110 trips per day, ride the Staten Island Ferry, which is operated by New York City's Department of Transportation.

A single ferry can carry as many as 6,000 passengers. In addition, there are a number of privately operated ferries such as the New York Waterway, which makes more than 1,600 trips per day carrying up to 31,000 passengers around the Port of New York and New Jersey. The Circle Line and NY Fast Ferry make 42 and 56 trips per day, respectively, carrying thousands of passengers. Water taxis make hundreds of trips per day between 14 pick-up and drop-off locations around New York and New Jersey.

II. The Terrorist Threat New York City's Mass Transit Systems

New York's extraordinary network of mass transit systems is the City's lifeblood. It is also, in most threat assessments, including my own, the single most likely target of another terrorist attack in New York.

We are aware of approximately 250 terrorist attacks on rail targets between 1998 and 2006. Most of these attacks have involved the use of improvised explosive devices against a passenger rail car. For example:

- In March 2004, a synchronized bomb attack occurred during the morning rush hour on Madrid's commuter train system, killing 191 and injuring over two thousand. Ten bombs detonated aboard four trains that passed through one of Madrid's main transit hubs.
- On the morning of July 7, 2005, terrorists targeted commuter system through a series coordinated attacks. Three underground trains and one bus were targeted. The attacks killed 52 commuters and injured close to one thousand.
- On July 11, 2006, a series of seven bomb blasts took place over a period of 11 minutes on the Suburban Railway in Mumbai, which like New York is a financial hub. More than two hundred people lost their lives and over 700 were injured in the attacks.

Mass transit systems present several distinguishing characteristics that combine to make them attractive targets for our terrorist enemies. Mass transit systems are inherently open systems thus, easy to enter. They are densely packed with people at predictable-times, and an attack against mass transit can have severe economic impact.

The threat to New York City's transit system is not just theoretical; it is real. There have been 22 bomb threats and 31 intelligence leads related to subway attack plots this year. The NYPD Transit responds to approximately 300 suspicious package calls per month.

In August 2004, shortly before the Republican National Convention, Shahawar Matin Siraj and James Elshafay were arrested by the NYPD for planning a bomb attack on the Herald Square subway station in Manhattan, not far from where the convention was to be held. During the spring and summer of 2004, these two individuals began to demonstrate increasing determination to attack the United States, transit systems in particular. Believing that an individual who was actually an undercover police officer would provide them with explosives, Siraj and Elshafay conducted pre-operational surveillance at the Herald Square station. In the spring of 2006, Elshafay pled guilty, cooperated the prosecution and testified against Siraj. Siraj was found guilty of conspiring attack the Herald Square subway. On January 8, 2007, Siraj was sentenced to 30 years in prison and on March 2, 2007, Elshafay was sentenced to five years.

Counterterrorism Operations in New York City's Mass Transit System

Responsibility for the direct protection of mass transit systems falls to local law, enforcement agencies and to the transit authorities that own and operate the systems. Many transit authorities maintain their own independent police forces or employ private security guards. Thus, multiple local, state, and private security forces are often involved in the direct protection of mass transit hubs.

At Grand Central Station, for example, the Metropolitan Transit Authority (MTA) Police Department provides security on the main concourse for Metro North, while the New York City Police Department secures the perimeter of the station and the subway lines and tracks. MTA Police and NYPD Transit Bureau police officers are at times supported by a detachment of New York State National Guard troops on state active duty. During periods of heightened alert, New York State troopers may be assigned to patrol and ride commuter trains.

At Penn Station, MTA Police provide security for the Long Island Rail Road, where they may be supplemented by New York State troopers during periods of heightened alert.

Amtrak Police patrol Amtrak lines with support from the NYPD, and New Jersey Transit Police provide security for New Jersey Transit lines. NYPD Transit Bureau officers remain responsible for securing the subway. The New York State National Guard also provides additional support at Penn station from time to time.

Of all the agencies involved in the security of New York City's transit system, the NYPD Transit Bureau has the largest area of responsibility and provides the greatest commitment of personnel. Nearly 2,700 officers are assigned to the NYPD Transit Bureau, which secures and polices the New York City subway system. Crime rates in the New York subway today are extremely low by national standards and are lower than the Citywide average crime rates. The NYPD's commitment of law enforcement personnel to the subway is a reflection of both our attack on conventional crime and our assessment of the terrorist threat to the system.

One way to measure the risk of terrorist attack is to look at which jurisdictions are willing to put up their own resources, rather than wait for federal funding. As you know, New York City has been spending hundreds of millions of its tax revenue dollars to fund counterterrorism activities.

The NYPD Transit Bureau plays a central part in counterterrorism operations in this high threat environment. The nature of the transit system, with its confined spaces, heavy mechanical equipment, and dense concentration of passengers, demands that these officers be prepared to act decisively with minimal supervision under the most extreme and dangerous conditions. Due to the sheer size of the system, the NYPD cannot cover all stations and all trains at all times. Therefore, the NYPD has developed a number of innovative counterterrorism tactics and techniques for use in the mass transit system. These techniques include:

- *Container Inspection and Explosives Trace Detection Program* The NYPD routinely conducts more than 300 explosive screening deployments per week throughout the subway and the Staten Island Ferry; the number deployments is increased during periods of heightened threat or concern. These screening operations consist of either a physical inspection of bags, briefcases, and other containers being carried into the subway, or an external swab of these containers for explosives residue using explosives trace detection equipment. The U.S. Court of Appeals recently the legality of these operations, after which the practice was adopted by the Massachusetts State Police.
- *Transit Order Maintenance Sweeps (TOMS)* The NYPD Transit routinely deploys teams of uniformed officers to conduct high visibility sweeps of trains for suspicious persons or packages.
- *Critical Response Vehicle (CRV) deployments* Every day, the NYPD conducts high visibility counterterrorism deployments of over 150 uniformed personnel to high risk areas in the City, frequently including mass transit facilities.
- *Underwater tunnel operations* The Special Operations Unit of the NYPD Transit Bureau patrols and inspects the underwater tunnels and ventilation facilities of the New York City subway every day, verifying that the alarm and access control devices at these sensitive locations are in working order. In addition, the NYPD Transit Bureau stations a police officer at the entrance of each of the subway's underwater tunnels on a 24/7 basis.
- *Radiological detection* Most NYPD Transit Bureau supervisors are deployed with advanced radiation sensors, and the Counterterrsim Bureau and Special Operations Division will from time to time conduct special radiological detection operations in the mass transit system.
- *Canine deployments* The NYPD Transit Bureau has an active canine program that is currently being expanded. More than a dozen canine units are currently in the program; the target strength of the program is 27 canine units. In addition to detection capabilities, the dogs also serve as a deterrent to both crime and terrorism.

The MTA and Port Authority Police Departments also conduct explosive detection operations in the portions of New York City's mass transit system for which they are directly responsible. In addition, the MTA is engaged in a number of different chemical and biological weapons detection pilot projects in the major mass transit hubs and is in the process of deploying an advanced CCTV, access control, and alarm at its major stations.

The New York City Police Department has also been centrally involved in a regional, multi-agency effort to enhance the security of Amtrak's Northeast Corridor (NEC). The NEC Working Group includes representatives from law enforcement agencies with jurisdiction along the Amtrak line between Washington, DC and New York. Members include NYPD (Intelligence Division, Transit Bureau, Counterterrorism Bureau), Amtrak, NJ Transit, PATH, SEPTA (Southeast Philadelphia Transit Authority), Washington Metro, CSX (freight trains), Baltimore Transit, Delaware State Police, Maryland Police, and other law enforcement agencies covering jurisdictions through which Amtrak trains travel. All members are on a group email list so that information can be disseminated in "real time." The Working Group meets quarterly and holds bi-monthly conference calls. The Working Group supports the

NEC Executive Group, which includes fhe top executives of-the agencies having a vested interest in the security of Amtrak and rail transportation.

As this brief summary should make clear, the NYPD and its partner agencies have mad an enormous commitment of resources to the security of New York City's mass transit system. We have no illusions, however, about the vulnerability of the system to terrorist attack or to the terrorists' intent to attack. We have done a great deal, but much more remains to be done.

The federal government, on the other hand, has done very little to improve the security of New York City's mass transit system. This is understandable to a certain extent as the federal government has no significant operational presence in the mass transit system and no particular expertise as to its workings. The one thing the federal government has done since 9/11 of course, is make grants to the mass transit system operators. The recipients of these grants, of course, welcome them.

However, given the severity of the terrorist threat to the U.S. mass transit system and the overall level of U.S. expenditures on homeland security and the war on terror since the terrorist attacks of September 11, 2001, the federal government's financial commitment to mass transit security has been virtually zero. The disparity between the federal investment in aviation security and federal investment in mass transit security is a national embarrassment.

IV. Analysis of Draft "Rail and Public Transportation Security Act of 2007"

Before reviewing the specific provisions of the draft "Rail and Public Transportation Security Act of 2007," it is worth noting that that the federal government has already been authorized by, law to do virtually anything it wishes in the general area of transportation security. In particular, the Aviation and Transportation Security Act of 2001 (ATSA), as amended, declares that of the Administrator of the Transportation Security Administration "shall be responsible for security in all modes of transportation" (Sec. 101).[1] In addition, under the terms of the ATSA, the TSA Administrator "is authorized to issue, rescind, and revise such regulations as are necessary to carry out the functions of the Administration." The ATSA also gives TSA Administrator the power to issue these regulations immediately, exempting them from all other statutory and executive regulatory requirements and "without providing notice or an opportunity for comment." This is one of the most sweeping, unconditional conferrals of regulatory and other executive powers in the entire U.S. Code, and it builds upon a wide and diverse range diverse range of other powers previously conferred upon the U.S. Secretary of Transportation, the National Transportation Safety Board, the Surface Transportation Board, and other federal entities.

Thus, strictly speaking, the executive branch is not deficient in any legal authority to act, directly or indirectly, in ways that it deems important for the security of the nation's rail or public transportation systems. My first observation about the draft Rail and Public Transportation Security Act of 2007, therefore, is that it confers no powers upon the federal executive branch that the executive dranch does not already possess.

Reporting Requirements The draft Act would, however, impose upon the federal executive branch a variety of different reporting and procedural requirements related to rail and public transportation security. The draft Act would require the Secretary of Homeland Security to:

- publish a nationwide "modal plan" (also referred to as the "National Strategy for Rail and Public Transportation Security");
- publish a "strategic information sharing plan"; and
- promulgate regulations that require state and local agencies and transit authorities to conduct vulnerability assessments and prepare and implement security plans for the various different transportation systems for which they are responsible.

From a legislative vantage point in Washington, these reporting requirements, taken in isolation, may seem appropriate, valuable, and not unduly burdensome. My vantage point has been from the executive branch, first in Washington and now in the field, so I take a different view.

Since the attacks of September 11, 2001, the field of homeland security has been gripped by a mania for plans, strategies, and other mandatory reports. I myself have been directly involved in drafting several such documents, such as the *National Strategy for Homeland Security* and the *National Response Plan.* In New York City, for instance, I personally am reviewing or contributing to about a dozen dif-

[1] The Homeland Act of 2002 superseded the Aviation and Transportation Act, vesting all powers and authorities assigned by the ATSA to the Secretary of Homeland Security.

ferent homeland security plans, reports, or strategies mandated by the federal government, often as, a condition for receiving federal grants. Most, if not all, of these documents are being written merely to fulfill federal requirements; they are of almost no value to operating agencies in the field; and they seem to be ignored by virtually everyone except the government contractors paid to verify the reporting requirements have been met—who are, in fact, often employed by the same companies as the contractors retained to write the reports the first place. For these reasons, I have become skeptical of the value of many these "national" policy documents. Too often, they reflect only the watered-down concensus of mid-level working group participants who have no significant connection to policy and operational decision-making of the most important agencies.

In addition, I do not believe it is reasonable to expect the Secretary of Homeland Security, or anyone else for that matter, to produce a useful comprehensive national strategy for securing all U.S. transportation systems. The complexity of the mass transit system in New York City alone boggles the mind. An attempt to generalize about the security deficiencies of all transportation systems in all parts of the United States—and to make meaningful proposals about how to remedy these deficiencies—is a complete waste of time. Since joining the New York City Police Department, I have learned how little Washington-based officials—as I once was—know about the real-world,, day-to-day activities of critical local transit authorities, and infrastructure operators. The sooner that the federal government, and the Department of Homeland Security in particular, realize that there are no "one-size-fits-all solutions in homeland security, the better.

For these reasons, I would recommend that the federal reporting requirements contained in sections 3 and 6 of the draft Act be pared back and the reporting mandate in Section 5 be stricken entirely.

Allocation of Grant Funds The draft Act would also authorize for appropriation substantial sums of money for various rail and public transportation security purposes, particularly grants to transit system operators. Specifically, the draft Act would authorize a total of $4.387 billion for transit security over 2008—2011, as follows.

Purpose	Amount (in millions)		Percentage
Rail Security	$600		14
Public Transport	$3,360		76
Bus Security	$87		2
Fire & Life Safety	$140		3
New York		$100	
Boston		$20	
Washington, DC		$20	
Security R&D	$200		5
Total	**$4,387**		**100**

I fully support the expansion of federal grants to non-federal security providers. I would note that the sums contemplated in the draft Act are substantially higher than those proposed in the President's FY2008 Budget, the Congress's Budget resolutions, or prior year appropriations in this area. The authorization of an expense does no good if the funds are never actually appropriated.

However, I have three major concerns with the particularities of the draft Act's grant authorizing provisions.

First, the draft Act fails to fund the single most important item for the protection and security of our mass transit system: daily security operations. According to the terms of the draft Act, the transit grants may be used only for "overtime reimbursement for additional security personnel during periods of heightened security as determined by the Secretary." This is unsound for a number of reasons. As I previously explained, the presence of well trained and proactive law enforcement personnel in the mass transit system is the most important defense against, and deterrent of, terrorist attacks on the system. These deployments should be continuous, not limited merely to the Secretary's, determinations of "heightened security." New York City operates in a period of heightened security all the time, irrespective of whether a federal announcement about a threat condition has been made to the media. The limitation of funding to overtime costs essentially penalizes the security agencies in high risk areas that deploy personnel into mass transit systems on a routine basis.

If the Rail and Public Transportation Security Act of 2007 is enacted as currently drafted, most of the funds authorized by this Act would, if appropriated, end up being spent on equipment and various services provided by contractors, not the agencies that actually provide security grant a day-to-day basis. This bias pervades virtually all homeland security grant programs. It is a reflection of the interests of government vendors, who sell more products, and federal auditors, whose jobs are simplified when grants can be connected to invoices. The federal government should rebalance its grant programs by shifting funds from equipment and contractor services toward operational security costs.

I recommend that the Committee revise the draft Act so that grants would be available to support ongoing security operations. Equipment and technological fixes are not the answer to mass transit security. The answer is people who can recognize threats and respond. The bill should allow grants to be used, subject to the approval of the Secretary of Homeland Security, to support not only the overtime expenses already in the bill, but also straight time and other ongoing personnel-expenses security to mass transit systems. This would be similar to the authority provided in the Fiscal Year 2007 Urban Areas Security Initiative grants, where personnel expenses for counterterrorism and intelligence are allowable expenses.

Second, even for the limited personnel expenses permitted by the draft Act (mainly training), the draft Act fails to recognize that the agencies conducting security operations in the mass transit system may not be connected to the transit authorities that operate the systems. The draft Act's definition of a "transit worker" is far too narrow, as it fails to recognize the diverse protection schemes needed to secure a transit system, which frequently crosses city, county, and state lines. In New York City, for example, the MTA is primarily responsible for operating the subway system, but the NYPD is responsible for patrolling and policing the subway. The draft Act would cover security training for the MTA employees—such as subway train operators, conductors, booth clerks, cleaners, property agents, etc—working within the transit systems or on MTA property, but the Act would not support security training for police officers assigned to the NYPD Transit Bureau (or specialized units such as the Emergency Services Unit, the K–9 Unit, or others) who are deployed to patrol subway stations, conduct random bag checks, and provide general security within the transit system. City, county, and state police agencies along Amtrak's Northeast Corridor contribute to the protection of this vital inter-city rail line, but their personnel expenses would similarly be excluded from the grant program due to the narrow definition of "transit worker." The Act should reflect the nuanced organizational structures that operate and protect transit systems to ensure all relevant non-federal institutions and organizations are covered by the grants this Act seeks to provide.

The bill should not limit training to employees of the mass transit system. Any person who provides to the mass transit should be eligible for training. In addition, in order to train someone, another person must fulfill the trainee's duties: The overtime and backfill costs associated with training should also be eligible for reimbursement.

Third, the draft Act fails to direct the Secretary to distribute federal transit security grants solely on the basis of terrorist risk. The draft Act would give the Secretary freedom to allocate the transit security grants on the basis of considerations other than objective assessments of terrorist risk. New York City's experience has been that the Department of Homeland Security frequently fails to incorporate these objective assessments of terrorist risk into its grant allocation decisions even when it has the statutory discretion to do so. The 9/11 Commission and virtually all independent experts and officials agree that terrorist risk is the only legitimate basis for allocating homeland security funds across the nation. The 110th Congress has the opportunity to do what the 108th and 109th refused to do—refused to do—incorporate terrorist risk fully into federal homeland security grant making processes.

Accordingly, the Committee should add to the draft Act a provision that directs the Secretary to allocate all grant funds authorized in the Act on the basis of objective assessments of terrorist risk, including the relative daily ridership of the mass transit systems.

V. Conclusion

I go to work every morning—frequently via mass transit—with the mindset that today will be the day that terrorists strike New York City again. The most likely scenario, I believe, is an attack in the subway system with multiple, near-simultaneous satchel bombs. The NYPD and our partner agencies have shouldered the responsibility for guarding against this horrific possibility. It is high time for the federal government to contribute in a significant way.

The Committee's draft "Rail and Transportation Security Act of 2007" is a step in the right direction, particularly in its authorization of grant funds at a level that begins to be commensurate with the true terrorist risk to our mass transit system. I urge the Committee to make the adjustments in the draft Act that I have identified in this testimony, and I urge the Congress to not only pass the Act but also to appropriate funds at the levels it would authorize.

Mr. THOMPSON. Thank you very much.

I think Ranking Member King will agree with me that we have tried on two former occasions to target the money where the greatest risks happen to be. But suffice it to say when it gets over to the Senate, it is a different matter. But we hear you. We understand it. And we agree with you.

I thank the witnesses for their testimony. I remind each member that he or she will have 5 minutes to question the panel.

I will now start with my questions first.

Mr. Fairfax, are you comfortable that the existing whistle-blower statutes managed by DOL serve a useful purpose?

Mr. FAIRFAX. Yes, sir, I am. The 14 statutes we enforce all provide protection, whether it is protection for workers complaining about safety and health issues or in the case of Sarbanes-Oxley, complaining about reporting financial misdeeds or, you know, AIR 21, which is the FAA dealing with airplane safety complaints. I think complainants need and must have a right to protect, file a complaint without fear of retribution. And I think all 14 statutes serve a very useful purpose.

Mr. THOMPSON. Thank you very much.

Mr. Hawley, can you give me TSA's position on whistle-blower?

Mr. HAWLEY. Yes, sir. We have, as you know, whistle-blower protection that is through the arrangement with the Office of Special Counsel. And that is a parallel system that we use and afford those protections to TSA employees.

Mr. THOMPSON. Do you know how many whistle-blower complaints have been issued under that process?

Mr. HAWLEY. I believe the answer is one from a transportation security officer and, I believe, something like 18 in total.

Mr. THOMPSON. Over what period of time?

Mr. HAWLEY. To be delivered to the committee. But I believe it is the—well, I will have to—not seeing any answer, we will have to get back to you.

Mr. THOMPSON. Well, so we go from 1,900 a year to 18? Do you think that is because employees are not comfortable with the existing manner that whistle-blower complaints are held?

Mr. HAWLEY. I have heard that opinion expressed. And I don't really—I can't say for sure eliminate that possibility. But it is something that is any TSA employee that has that we have a number of avenues to raise concerns, both within TSA and outside of TSA. And if there is anybody with any doubt, they should come forward. And there is no retribution. And there are protections against retribution.

Mr. THOMPSON. So if we formalized the whistle-blower process as proposed in this legislation, where is TSA on it?

Mr. HAWLEY. We would certainly work with the committee on it. There are maybe some technical issues, but I think that is something we would support generally. And my numbers, I am told, are 12 non–TSOs, one TSO in the last 2 years.

Mr. THOMPSON. Thank you. And I think some of us think that if we had a more robust system to allow people to make complaints we probably would have more. I think the fact that we don't has a chilling effect on employees.

The other issue, Mr. Hawley, I have: How has your relationship been with DOT as you deal with matters of security?

Mr. HAWLEY. I think very close. And we have, as we mentioned, we brought Robert Jamison, who is the former deputy from DOT, deputy administrator and acting rail administrator. And we have MOUs. We deal closely with Mr. Rosapep and his colleagues at FTA.

Mr. Rosapep mentioned the December meeting of the roundtable. It is something that I attended and FTA is—actually the FTA administrator attended. So we have both formal and informal processes we work together. And I think all of us agree TSA does security, and DOT does safety. And we understand those roles and support each other.

Mr. THOMPSON. Thank you. My comments in my opening statement talked about a report that was overdue. Can you tell us where we are now?

Mr. HAWLEY. Yes, sir. It is still under review. And I accept whatever comment you would care to make on that. It is late. And the work is done. I think there used to be a time at TSA when our words were ahead of our actions. And I am pleased now that our actions are well ahead of our words. And we have got quite a lot of things we have actually done that reflect the work that went into those reports. And I very deeply regret that the reports are not here for you to review at the same time.

Mr. THOMPSON. And you are aware that report is 3 years overdue?

Mr. HAWLEY. Well, all I know is it is extremely overdue. You are, no doubt, correct.

Mr. THOMPSON. You take my word for it?

Mr. HAWLEY. I absolutely do.

Mr. THOMPSON. Okay. Thank you.

Ranking Member King?

Mr. KING. Thank you, Chairman Thompson.

I would ask all the members of the panel—you probably heard the dialogue between myself and Chairman Thompson at the start about the funding for these grants remaining with the Department of Homeland Security. Could each of the four you tell me where you stand on that issue?

Mr. HAWLEY. We are in agreement with that position. DHS, the secretary—I think I can speak on behalf of the secretary.

Mr. ROSAPEP. At DOT, we support that as well. We think it is important that transit security really be part of the overall security approach of states and local areas. And it is important that transit security be addressed really within that overall context. And DHS has a full range of programs that address all aspects of security. And we think it is important that transit stay within that mix.

Mr. FAIRFAX. We certainly support the department's for its transportation security. And we are still studying the bill. And our only aspect is the whistle-blower provision of it. And we are still looking at that and trying to figure out the scope of it.

Mr. FALKENRATH. We think the money should stay with DHS. We have a difficult enough time dealing with DHS on these monies. The arrangements of who deals with them internally at DHS have changed a lot in the last couple of years. We don't need more change. We need to settle down, get a little bit of continuity in this arrangement so that we can develop the working relationships we need and get on with business.

Mr. KING. Thank you. Also, I know Mr. Perlmutter is not here. And I just would like to ask Mr. Hawley and Commissioner Falkenrath—we will make available copies to you of his amendment which passed last week regarding protections for employees as to when they can be dismissed, et cetera, as to whether or not you think that would interfere with operations and secondly, whether or not you believe that that would preempt state and local officials from taking appropriate action against employees.

Again, Mr. Perlmutter is not here. I don't profess to be an expert on the amendment, but I would appreciate if before we have our markup next week if you could get back to us with an opinion on that as to how you feel the impact upon both the national level and also at the local level. And again, I am not reflecting Mr. Perlmutter, although I do have some concerns, though. And I would like to see them addressed by the department and by the NYPD.

Mr. HAWLEY. Sure. This has been an issue that has come up in a couple of contexts. And we have issued in our transportation worker identification credential a card, so to speak, a set of legislatively and, you know, criteria that have gone through a rule making process to lay out what the crimes are, that there is a 7-year cooling off period, if you will, for some crimes. Some are permanent bars.

And there is an appeal process and a redress process that is built in. So we have written those up and put those out to the public for those wishing to do other background checks, particularly in the private sector. And we believe that is enough to support our federal needs for security, those background check guidelines.

Mr. KING. Well, again, if you could get back to us, though, before next week with an analysis of the amendment.

And, Commissioner Falkenrath, I know you haven't seen it. But if you could just have someone in the department take a look at it and get back to us on it.

Mr. FALKENRATH. We will, sir. Although we are against the preemption of state and local authorities—that is clear.

Mr. KING. Right. Again, and I don't want to—I mean, that is my characterization of it. So I am not even, you know, asking you to accept that. I wish you would take a look at it and see if you agree with us on that.

Commissioner Falkenrath, in the minute-and-a-half that I have left, you raised issues that you and I have discussed obviously about the whole issue of funding as far as personnel. And I am in basic agreement with you. What we can do as far as getting this through the House and through the Senate in the form that you and I would like is another question.

But you did raise the issue that right now the legislation seems to be geared towards just transit employees. And you are right. In New York, most of the actual transit security work is done by prob-

ably non-transit employees. It is done by NYPD. It is done by the MTA police and the Amtrak police. If the training money was also allocated to police as opposed to just transit employees, do you think that would make a significant improvement over the legislation?

Mr. FALKENRATH. I think that is one improvement that should be made in the legislation. I mean, as you know, the NYPD Transit Bureau used to be a separate agency.

Mr. KING. Right.

Mr. FALKENRATH. Part of the MTA essentially. And it was reorganized in 1994. And so, that fact just has to make its way to that bill to understand that there have been reorganizations.

Mr. KING. I believe you said there is about 2,700 cops in the transit division.

Mr. FALKENRATH. Yes, sir. And now up and down the Amtrak corridor we have regular meetings with all the Amtrak security agencies. Local state police departments are providing security for the Amtrak Northeast corridor. They would be excluded as well. So it is not just NYPD. It is all the law enforcement agencies that contribute to this mission that just happen not to work for a transit agency.

Mr. KING. I assume that the MTA Commissioner Bill Morange would also agree with you on this?

Mr. FALKENRATH. I believe so.

Mr. KING. Yes.

Mr. FALKENRATH. They actually speak for themselves. But we have an excellent working relationship.

Mr. KING. Right. Okay.

And my time is expired.

Mr. Chairman, I do think Commissioner Falkenrath does raise a very serious issue, though, as far as the training. Training is essential, but it would be going really largely to people who are not involved in the day to day security work on the mass transit.

Thank you. I yield back.

Mr. THOMPSON. Thank you very much.

I now yield to the gentlelady from California, Ms. Harman.

Ms. HARMAN. Thank you, Mr. Chairman and Ranking Member King.

I strongly support this legislation and this focus on transit security. And I think the testimony this morning was very helpful.

Let me first say to Mr. Hawley, I appreciate your responsiveness. You have a very big job. Not every decision you make is wildly popular up here. But I have found that you are open and try to deal with member questions fairly. And I really appreciate the effort you have made in the Los Angeles area to try to match resources with needs. So I want to thank you for that.

I also appreciate your strategic approach to problems. There is no such thing as 100 percent security. I think everybody knows that. What we all have to do is manage risks and be as strategic as possible. And I think you are trying to do that. So thank you, on behalf of a grateful member on this committee.

Mr. HAWLEY. Thank you.

Ms. HARMAN. To Mr. Falkenrath, I would point out to members they may notice that before you moved to this important role at the

NYPD, you were working at the National Security Council or the White House. Or which was it? Both. And with a think-tank in between. So you have seen this problem from both ends. Therefore, we can hope that you are very mindful of the perspective we take here as federal legislators trying to get this right from the federal perspective.

But you are the one I want to ask some questions to. Three of my four children live in New York. Two of them are regular riders of the subways. Millions of other New Yorkers do the same thing. This mother worries all the time. In fact, I got into an argument with Mayor Bloomberg because I said the subways were vulnerable, something you just said. So now maybe you will get into an argument with Mayor Bloomberg.

But it is critical that we do our best to have a strategy to protect millions and millions of subway riders in New York and elsewhere, certainly not just my kids. And you have testified to the steps you are taking. You have also made some suggestions about how we could change some features in this bill to make it more effective.

But my question to you—and maybe it is to others, too—is what role does intelligence play in this whole effort. Surely, funding matters. Surely, funding to transit workers matters. But if there is no such thing as 100 percent security, what do we really need to do? And should we think about it in this bill or in other steps we take to maximize learning in advance about threats to our mass transit systems from hopefully specific places or specific individuals whom we could then target effectively?

Mr. FALKENRATH. In my opinion, it is immensely important. In fact, intelligence in our law enforcement investigations are probably our most important line of defense against an attack on New York City subway. Once a plot is formed and the weapon is in their hands and they are just walking into the place to set it off, the advantages have all gone to the attacker and not with us. So the intelligence is enormously important.

I think you know about our program. We take that part of the mission pretty seriously, too, both in the context of the FBI joint terrorism task force and unilaterally. So we pursue that very aggressively.

The tip line that was mentioned earlier is in every subway car. You can see a number to call. That number will be answered by an NYPD detective. And every single lead will be run down without fail. And we get a lot of leads in the subway off of that. Some of them are referred to the JTF, but most are not. And that intelligence is very important.

Our protective measures that we deploy, which I enumerate in the testimony, are all intelligence driven. And we put them in places where we deem important for one reason or another. We just don't have the resources to cover the breadth of this system. I understand your issue with the subway security as a mother. I also ride mass transit to get to work frequently. And it is a worry. It enters your mind when you are there, there is no question about it.

Ms. HARMAN. Would others like to comment on the value of intelligence and any steps that we should be taking, specifically focused on mass transit security that we are not or additions to this legisla-

tion that you would recommend focused on getting accurate national intelligence?

Mr. HAWLEY. I think the legislation—one of the strong points of the legislation is that it hits that point exactly very hard in terms of information sharing and the importance of intelligence. And I would like to support what Commissioner Falkenrath said and particularly the point you made about strategic intelligence that if the target is America, finding out when the plots are being set up prior to, as Commissioner Falkenrath says, they start showing up at our targets, if you stop them way back in the process, that is the way to do it. And that happens with sharing of information.

Ms. HARMAN. Thank you.

My time is expired, Mr. Chairman.

But this is a subject obviously that our committee will continue to probe. Thank you.

Mr. THOMPSON. Thank you very much.

The gentleman from Connecticut, Mr. Shays?

Mr. SHAYS. Thank you very much, Mr. Chairman. Thank you for conducting this hearing with the ranking member.

I would like to first ask any one of you what you think the strategy to deal—well, let me first—the strategy to deal with the Cold War was contain, react and mutually assure destruction. What is our strategy to deal with terrorism?

Mr. HAWLEY. It is proactive, and it is network-oriented. And I think as Congresswoman Harman was saying, it has to start off at the strategic level, which is to say that the target is the U.S. and our allies and to start to push it as far back as possible and fight it in layers every step of the way. And this relates to the transportation security agency. Our role is looking at the transportation networks, all of them that connect in the United States and then having our layers plug into efforts that are already in place and be as proactive as possible.

And I think Commissioner Falkenrath hit it right on the head in saying that it starts at getting the intelligence at the ground level from citizens who are the eyes and ears. And it goes all the way up to the foreign intelligence and military.

Mr. SHAYS. Thank you. I am very comfortable with that response. It is proactive instead of reactive. And I like the concept of networking. If I said to you it is to detect, prevent, preempt then maybe to be unilateral, are you uncomfortable with any of that description?

Mr. HAWLEY. Only unilateral. I think it is—

Mr. SHAYS. Let me ask you if a small group of dedicated scientists were creating a biological agent that would wipe out humanity as we know it, do you think even Jimmy Carter would wait to get permission from anyone to deal with it?

Mr. HAWLEY. Well, I am referring to my partners in terms of none of us in the U.S. government work alone is really what I was referring to.

Mr. SHAYS. Got you. Okay. Went to Great Britain after they made the arrests of the individuals who were going to hijack the airplanes and come into the United States. When I met with Scotland Yard, I said did homeland security have anything to do with

these arrests because homeland security took some credit. And they said absolutely not.

Then I was at 10 Downing Street meeting with the advisers to Tony Blair. And I said did homeland security have anything to do with it. And he said a lot. And it was really kind of cool because what it said to me was the people who needed to know knew, and the people who didn't need to know didn't know.

And that gets into your sense of networking. Do you think we are safer today than we were before September 11th, any of you?

Mr. HAWLEY. I would say without question.

Mr. SHAYS. Yes. Why do you think people don't feel we are safe?

Mr. HAWLEY. I am not sure they don't. I think that the travel levels have recovered beyond what they were prior to 9/11. And I think the degree of connectedness both among parties in the U.S. government with the state and locals and with other partners across—

Mr. SHAYS. Polls state that they think that we are much less safe.

Mr. HAWLEY. I beg your pardon?

Mr. SHAYS. Polls will state that they think we are much less safe. And what is shocking is that even the experts feel that way, the outside experts. Any—

Mr. HAWLEY. Not this one.

Mr. SHAYS. Well, anybody?

Mr. HAWLEY. I can't speak for the poll. I haven't seen that polling data. My personal opinion is we are substantially safer than we were on September 10th.

Mr. SHAYS. Yes. Don't you think the reason they don't feel as safe is they had a false sense of security before September 11th? In other words, people just really didn't think there was a problem. And now they know there is a problem and they don't feel as safe, even though, in fact, they are safer. I mean, I would agree that they are safer.

If you give the administration more power, what do you think—and more power to do things that would seem invasive to civil liberties, what is our solution to that?

Mr. HAWLEY. I don't see us lacking authority to do our job at this point. And I think in the committee bill there are some additional clarifications that help us enforce the authority that we do have that further close the loop. So I think we do have the administrative tools.

Mr. SHAYS. Right. But my point in asking the question is the administration has been given more authority. You all have. Which means that we need to have greater congressional oversight to make sure it is not abused. One of the most important ways to do it is to have a workable whistle-blower statute.

And the thing that troubles me with the punishment of whistleblowers is that their insecurity is the first thing that is taken away from them is their security clearance, which is like going to a bus driver and saying you don't have a license to drive a bus. Is there anything, in the 5 seconds here, that speeds up the process of determining the validity of what a whistle-blower tells us?

In other words, it takes so long. Is there any way that we speed up the process to determine the validity of what the whistle-blower is saying?

Mr. FAIRFAX. We have been struggling with trying to speed up the process for years and haven't really been successful. You know, the investigative process requires us to interview the complainants, the respondents, their witnesses. When different statements are made, we have to go back and reverify and double check the data. So the process takes a long time. And we have been struggling, like I said, with it and have not been able to shorten that timeframe down.

Mr. SHAYS. Thank you, gentlemen, for your service to our country. I appreciate it.

Mr. THOMPSON. Thank you very much.

I now go to the gentlelady from the District of Columbia, Ms. Norton.

Ms. NORTON. Thank you very much.

I guess this is for Mr. Hawley. Mr. Hawley, I sponsored with the support of many in this committee a comprehensive rail security bill in the last Congress. There was great frustration that this remained an area where Congress had not tackled. You or TSA has issued proposed rules. And one of its provisions would bar state and local jurisdictions from engaging in rerouting of hazardous materials.

Well, it is understandable. It is a federal responsibility. But in the absence of any federal action, despite the fact that hazardous substance trains run literally within a stone's throw of this building and other federal buildings, the local jurisdiction and the District of Columbia on its own filed a suit.

The fact that that suit is still being heard in the Congress tells you it was not frivolous. The reason it was not frivolous is that despite your authority under the commerce clause, when it is not exercised, the courts have held that a local jurisdiction doesn't have to just sit there and be hit. And so, it is still being heard.

You have proposed regulations that essentially are inspection regulations while the train is not moving, do a thorough inspection. My question to you is particularly in light of the way in which trains have been attacked in Europe and elsewhere, is it your view that trains are not likely to be attacked when they leave their station, as it were? You even propose that notice be given to locations that information that hazardous substances may be going through the jurisdiction so that local jurisdictions could take the required action.

Why one? Why not say notice or something that is required probably wouldn't be difficult to do because the trains probably come rather on schedule? And if not rerouting—and I am one of those who thinks you can't reroute very many places.

I do think there are parts of the country where the population is so dense or places like your nation's capital where you might want to do some rerouting. But why have you not therefore come forward with alternatives to rerouting other than inspections in place, which do not, of course, count or leave terrorists free, I suppose, to do their work on—to work their will when the train is in motion?

Mr. HAWLEY. I respect the question. And I know that in the second panel there will be more chance to discuss this from the railroad operator point of view.

But the specific answer to your question on why no notice is that the current system is that the municipalities are, in fact, informed of the kinds of materials that are moving through. The reason we did not require notification on specific shipments has to do with security in that there is an irregular pattern of these shipments which adds to the security level and that you can't plan exactly when and where one of these TIH cars is coming in if you are on the other side.

Ms. NORTON. You are saying—I am sorry—they do inform local jurisdictions when—

Mr. HAWLEY. Not the when, the what. They say we are moving this kind of material through your city. But they do not say and we do not suggest that we require exactly when a particular car is coming because—

Ms. NORTON. I am sorry, they are moving it through your city, you know, sometime this year?

Mr. HAWLEY. It says—

Ms. NORTON. If it doesn't say when, how could local jurisdictions prepare in case there is a problem?

Mr. HAWLEY. Well, local jurisdictions are able to prepare in terms of the first responder as well as work with the security agents of the given railroad. But it is a security vulnerability to be passing out the information of the exact movements of TIH cars. So we do not believe that that adds to the security. We believe that actually makes it more vulnerable. So we have the capability as do the railroads—

Ms. NORTON. So you think if you were to supply that information to the local police chief or the local fire chief that the District of Columbia and New York City would be more vulnerable than it is now with no such information?

Mr. HAWLEY. Not at all. It is not the police chief or the fire chief I am worried about. But it is the more widely that information is spread around, the—

Ms. NORTON. Well, who is asking for it to be widely spread around? Again, I understand your security concern. There are also in every local jurisdiction people who have the appropriate clearance. And so, I don't understand that to protect security you are making local jurisdictions less secure by not giving them information that is necessary.

Mr. HAWLEY. It is like passing out the flight plan for Air Force One. That is not something that is out there.

Ms. NORTON. Even if you give that information to those officials who have the needed security clearance—and there are such officials in every jurisdiction.

Mr. HAWLEY. Absolutely. On the security clearance, that is another issue that we do completely share.

Ms. NORTON. Thank you, Mr. Chairman. That is why we are in court.

Mr. THOMPSON. And that is why we will have a rail bill to mark up.

That is an issue, Mr. Hawley, I want to assure you. In the absence of a policy when local officials become proactive on behalf of their citizens and then for our government to tell them that they should not become proactive in the protection of their citizens, that is a concern. And obviously I understand the policy. But we have any number of local officials who come with that very concern.

We will now hear from the gentleman from Washington, Mr. Reichert.

Mr. REICHERT. Thank you, Mr. Chairman.

Mr. Hawley, I come from the Seattle area. We operate quite a large ferry system. What grant program provides assistance to the ferry system as far as security goes?

Mr. HAWLEY. There is a port grant program that is administered by the Coast Guard.

Mr. REICHERT. Coast Guard has a separate grant system?

Mr. HAWLEY. Yes, sir, the port security grant.

Mr. REICHERT. I want to go back to Mr. Falkenrath's comments. I was a sheriff in Seattle up until about 2 years ago. But the things that you said really struck a note with me. From the local law enforcement perspective, we know that there is enough rules and regulations.

We know there is enough bureaucracy that we have to go through as local law enforcement officers. We know that reporting requirements are cumbersome. And, you know, it does seem to be a waste of time for us to assign resources to that.

It seems to be at the benefit of bureaucrats and politicians rather than really getting at the heart of what the problem is and us trying to get our job done on the street as cops, firefighters, and emergency managers and others of those who are out there protecting our country. And it sometimes gets very disappointing that the federal bureaucracy gets in the way.

I do agree that personnel costs must be a part of the grant program. We are working toward that. There are other types of agencies that are involved in working with transit authorities, other law enforcement agencies and emergency managers that do come into play. And it should be based on risk.

Now, all of you did say that, you know, you support still the idea and concept of the Department of Homeland Security managing grants. But I would like to just get into it a little bit deeper. Why is it important for the Department of Homeland Security to oversee, not only the prioritization of grants, but the distribution and the monitoring of grants?

And, Mr. Falkenrath, maybe you could answer first.

Mr. FALKENRATH. Well, as someone who was involved in establishing the Department of Homeland Security, the concept then—and I think it is still valid—is you needed to integrate all the federal government's different programs to accomplish this mission otherwise it was simply too complicated for a state and local agency to deal with all the different parts of the federal government. They couldn't.

Now, I must tell you this Department of Homeland Security has a ways to go with integrating its different programs. It is not just the Coast Guard's port security grant for which you can apply for ferries. It is also the TSA administered transit security grant. That

gives money to ferries, too, totally separate application, totally separate working groups, totally separate people coming to the meetings. And so, that is our reality.

On the reporting requirements, though, sir, you will note that in your own bill it makes provisions to provide technical assistance to the state and local agencies for fulfilling these reporting requirements. Btu what that is is that is contracts for government contractors, who are then the same ones, I think, who read the report. So it is almost like a self-licking ice cream cone.

And the writing of these reports is, in my judgment, very poorly linked up with any sort of strategic risk assessment that is rigorous and sound and with operational day to day decision making. So my judgment is that I am not against them per say. I, in fact, believe with the author of the HSPD that required the drafting of the report that is now 3 years overdue. You know, I have been on both sides of this. But I think it is excessive.

Mr. REICHERT. Yes, I would agree.

Mr. Hawley?

Mr. HAWLEY. Just picking up on the back to the Seattle ferries thing, that that is a reason itself. We have a $7.5 million in transportation security grant program of which ferries are eligible. And in this year's meeting Thad Allen, the commandant of the Coast Guard, and I were in the same meeting.

We were talking to have the whole effect of all of the DHS money to hit what the same vulnerability risk assessment to make sure that we were hitting, regardless of which arm was handing out the grant, that it was a connected strategy at the top. And I think that is the critical piece, that it all starts with the risk look at threat vulnerability and consequence across the whole nation. Infrastructure protection, transit, port, all of these are driven by the same risk assessment.

Mr. REICHERT. Wasn't the whole concept behind grants and trainings and homeland security a one-stop shop for those first responders? Anybody?

Mr. HAWLEY. It was a concept. It is not the current reality.

Mr. REICHERT. Is that the goal?

Mr. FALKENRATH. I have actually myself come to question the wisdom of that concept because I have seen how it went in the one portion of the Department of Homeland Security that did consolidate control over several of these grants. And frankly, we were dissatisfied with that outcome as well. So it is sort of six-and-a-half dozen at the moment.

I just would—I think, though, it would be imprudent to bring yet another cabinet department in. You know, at least in this case we have one deputy secretary and one secretary who oversees it all. It would be another if the only person who oversaw them all was the president of the United States.

Mr. REICHERT. Thank you, Mr. Chairman.

Mr. THOMPSON. Thank you very much.

I now yield to the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Gentlemen, thank you for your testimony here today.

Mr. Hawley, I will start with you. I know you all have a very difficult job to do. And we appreciate your service to the country. I want to start out by asking what is it that keeps you up at night.

In your area of responsibility, what is the thing that you are most worried about? And do you feel, in your opinion, that you and your department have done everything you can to close and address that vulnerability, first of all?

Mr. HAWLEY. Well, I think my biggest concern is it gets back to the issue on the strategy, which is connecting all the pieces from the person on the subway car to the detective answering the phone to the intelligence officer who might be abroad, to have all of us connected, that there might be some piece of information out there. And the 9/11 Commission talked about connecting the dots.

How do we make sure that of all the information coming in that we process fast enough the information and get it to the people who need it, particularly on the ground and in the New York City case? Because they are not federal officers on the ground, that we make sure the NYPD has the information when they need it and vice versa, that they get it to us in case there is some kind of a network aviation problem or something. So it is that information sharing.

That is I have actually oriented my day. I spend the first hour of every day working on the intel side with all the intel agencies of the U.S. government and law enforcement and then converting that to the TSA team to what actually are we doing about it, what information could we share with the other partners in the work. And that is the real work of what we do.

And as I said earlier, we are behind in writing our reports. We are absolutely not behind in getting on top of information and sharing it.

Mr. LANGEVIN. Let me turn to transportation security with respect to rail. On average we spend $9 per air passenger annually on security and only one penny per rail in mass transit passenger. And while we can all agree that our rail and mass transit systems are far from secure, the president's fiscal year 2008 budget only calls for only $41.4 million out of a $6.4 billion to be spent on rail and mass transit security. So this is only a 1 percent increase from fiscal year 2007, which doesn't even keep up with inflation.

The administration's proposed budget is, I think we can agree, far from adequate to close many of the existing gaps. So, Mr. Hawley and Mr. Rosapep, in terms of rail and mass transit security, where do the biggest gaps remain? And have your respective departments come up with specific plans to address these threats? And what are your priorities in terms of closing many of the existing gaps?

Mr. HAWLEY. I would say in the transit area, I mentioned at the beginning it is underwater, underground tunnels and, yes, adjacent or in highly dense areas. And when you boil it all down, it gets to the fundamentals of training and public awareness and emergency response.

And one of the reasons that we don't spend more money at the federal level is because of the feet on the street and the work that NYPD does and others across the country at the local level where the state and locals pick up the people there, which is why they

absorb the budget and we in the federal government absorb the airport environment. So it is truly not an apples to apples.

And I think we look at threats and risks at the total system perspective and we don't really say we are going to focus on aviation or focus on transit. We focus on the whole country.

Mr. LANGEVIN. Mr. Rosapep?

Mr. ROSAPEP. We agree from the department's standpoint with the priorities that Mr. Hawley laid out, again, in terms of the need to provide additional training and emergency preparedness planning for particularly the transit agencies. F.T. does not have its own security grant program. But we can redirect and are redirecting some of our internal resources to put more money into the training programs that we develop and deliver.

And another provision under the last transportation reauthorization bill does allow transit agencies to use some of their capital transit dollars for what are more operational expenses, such as paying for training, developing preparedness plans and conducting drills. So those are areas that we are trying to reinforce with our grantees.

Mr. LANGEVIN. I see my time is almost expired. But I want to reiterate that, you know, when we are spending $9 per air passenger annually and only basically one penny per rail and mass transit passenger, in my opinion, we are not doing enough in the right areas to protect our rail system, particularly our passengers. We need to redouble those efforts. It is only a matter of time, in my opinion, that is going to be a target. And we need to do better than what we are doing right now.

Thanks, The CHAIRMAN.

Mr. THOMPSON. Thank you very much.

We now yield to the gentleman from Pennsylvania, Mr. Dent.

Mr. DENT. Thank you, Mr. Chairman.

Mr. Hawley, good morning.

Mr. Hawley, a question for you. Could you describe the national security impact, if any, in transferring rail security, mass transit and over the road security transits out of the Department of Homeland Security into the Department of Transportation?

Mr. HAWLEY. I think the primary issue is the connectedness to the overall risk assessment we have that is done at the DHS level and that coordinating the forces that we have and the money that we have to hit the center of the target. And we feel that that is best done from the security point of view at DHS and certainly the safety area is DOT. But we work very closely. We have an MOU with DOT to that regard.

And I would like to thank the Allentown and Bethlehem Airport for lending us Dempsey Jones to the federal security directorate to lend to Jackson, Mississippi for a period. So thank you.

Mr. DENT. You are welcome.

Mr. THOMPSON. Good man.

Mr. DENT. Most welcome. And my second question deals with this. The rail and mass transit security bill that proposes to make it a criminal offense for a supervisor to retaliate against an alleged whistle-blower.

Given that supervisors often have to make difficult decisions that sometimes irritate their employees, do you think this provision will

have a chilling effect on managers who have to make unpopular decisions for fear that they could be accused of retaliation against those claiming to be whistle-blowers? And, you know, will we now have to provide Miranda warnings to managers and supervisors in light of the fact that what they say in the course of their duties could possibly land them in jail?

Mr. Fairfax?

Mr. FAIRFAX. Okay. Well, we are still studying the whistle-blower provisions of this bill. But the scope in how we do investigations doesn't really, I don't think, lend itself to that concern. But we have a fair investigative process. I don't think there is a chilling effect on supervisors when we do the investigations. They are allowed to bring forth their witnesses.

We interview them. We interview all their witnesses. We interview the complainants and the complainant witnesses. That is part of why I was saying earlier, the process takes so long is there is a lot of, you know, discussion, documentation, verification, reverification. And only about 22 percent of our cases end up being merit against an employer once we have gone through the whole process.

Mr. DENT. You don't have any major concerns then about this? I think that is what I heard, about those criminal provisions in the real security bill?

Mr. FAIRFAX. No. We have those in areas like Sarbanes–Oxley and such.

Mr. DENT. Okay.

Anybody else? Okay.

I yield back the balance of my time. Thank you, Mr. Chairman.

Mr. THOMPSON. Thank you very much.

I now yield to the gentlelady from New York, Ms. Clarke.

Ms. CLARKE. Thank you very much, Mr. Chairman. I want to first of all just thank you for sponsoring and shepherding this very important piece of legislation. I also want to thank Ranking Member King for his commitment and resolve to get this system right through bipartisan cooperation.

I would like to also extend my thanks to Chairwoman Jackson Lee and Ranking Member Lungren for their hard work on this bill.

The Rail and Public Transportation Security Act of 2007 takes a major stride in the security of America. This bill authorizes more TSA officials to better secure ground transportation, increases the number of transportation security inspectors, and creates a research center to study future solutions, calls on transportation providers around the country to do what New York has already done and create a detailed security plan to ensure the safety of passengers.

Further, this bill creates a security training program, which will train employees of all covered transportation carriers to know what to look for and how to react should a security situation arise. The women and men working in our subways, railroad stations, bridges and tunnels are our first line of defense. For example, if an unusual package sitting in the New York City subway is detected and acted upon early enough, countless lives will be saved. Or if there is an explosion in a tunnel, maintenance workers may well be on the scene even before the police.

A proper evacuation may again save lives. Through this bill transportation providers will be able to team with labor unions to ensure employees are trained to deal with these scenarios. However, I do believe that this emphasis should not preclude law enforcement personnel from being recipients of funding through this provision.

Finally, I again want to thank Chairman Thompson and Ranking Member King for their efforts to include $100 million in funding for safety upgrades to Penn Station in New York City. This much needed improvement will dramatically improve conditions for countless New Yorkers and visitors to our city.

You know, I heard Congressman Shays raise the issue of a false sense of security and vulnerability. And I have to tell you that as a New Yorker whose father is a Port Authority employee and was in the twin towers in 1993 and who continues to mourn the lives that were lost on 9/11, the sense of security is always shaky. But we know that life goes on. And securing our nation will always be a work in progress.

As a former member of the New York City Council, I am keenly aware of the financial strain our municipality continues to bear as a result of being the number one terrorist target of our nation and being constantly under the threat and having always to be in a state of readiness.

My question is to you, Mr. Falkenrath. You have discussed that New York City would like more flexibility in how it can spend federal grant dollars on overtime pay. Please give us some idea of what type of situation has caused New York to pay overtime for police and other first responders where it would not be able to use the funds contained within this bill.

Mr. FALKENRATH. Thank you, ma'am. The main program we call is called operation atlas. It is a counterterrorism program by which we take large contingents of uniformed officers and deploy them around the city in highly visible counterterrorism operations to provide immediate presence and to provide a deterrent effect on anyone who may be conducting a casing operation.

As you may know, New York City has been repeatedly cased by al-Qa'ida operatives and their affiliates. We know this with certain knowledge. Several have, in fact, been indicted and convicted in federal court or in British court for these exact activities.

And we learned from that that we need to provide a highly unpredictable and highly visible law enforcement presence around the city at key targets that may be cased from time to time. This is a part of Al Qaida trade craft. So that is what we do. And we pay for that for the most part out of overtime, which is very expensive.

As you know, we are 5,000 cops less than we were on 9/11 in New York City. And yet we do even more than we did at that point.

Ms. CLARKE. Mr. Chairman, I think that it is really important that, you know, we look at how we are utilizing the funds in this regard. New York City can provide a model for other vulnerable regions around this nation. And they have set the trend, but at extreme cost to our city. And I hope that we can show some appreciation for the level of intelligence and the level of skill that has been

developed as a result of this particular region of our nation having been going through these terrorist activities.

Thank you very much, Mr. Chairman. And I yield back the rest of my time.

Mr. THOMPSON. Thank you very much. I don't think there is any question about New York's standing in this whole discussion. The Ranking Member and I have had a number of discussions. And hopefully we won't have any surprises in the future with cuts in money and the like because we understand the gravity of the situation.

I have been to New York with the then Chairman and saw firsthand the situation. I met with Commissioner Kelly. I applaud New York for stepping up, obviously, because there is no federal standard. So it is really a state and local issue at this point. And that is why we are trying to move this issue forward.

Thank you very much.

I now yield to the gentleman from Florida, Mr. Bilirakis.

Mr. BILIRAKIS. Thank you, Mr. Chairman. Thank you. I am pleased to be here this morning to continue our examination of rail and public transportation security legislation. Before my questions, I just want to say that I think the bill we are here to examine is a reasonably good bill at which some alterations could be better.

I was pleased last week's subcommittee markup was largely bipartisan due to the open-mindedness of Chairwoman Jackson Lee and Ranking Member Lungren. I hope that the spirit of bipartisanship prevails during next week's markup as this committee addresses issues that concern me and many of our colleagues, specifically, how best to maintain the primary role that DHS plays in transportation security, protects sensitive information from public disclosure, and provides sufficient flexibility in the conduct of background checks on transportation employees.

My first question is to Mr. Hawley. In your written testimony, you said that current aviation security measures provide a significant barrier to entry for potential terrorists coming to our country. You further stated, "Our government's investments in improvement in terrorism watchlists, border security, and intelligence networks significantly enhanced service transportation security."

Would you please explain what type of screening or pre-screening, if any, is currently being conducted on freight and passengers that cross the border by rail?

Mr. HAWLEY. Sure. On cross-border transportation on freight, it is principally done through Customs and Border Protection, which has its own system there that is integrated also with ocean-borne freight coming into the United States. And they are the same authority on passengers when they are coming into the United States to make the decision whether they come in or not. So it is really not a TSA thing at the border.

Mr. BILIRAKIS. Okay. How is this similar or different from screening measures on air passengers and cargo?

Mr. HAWLEY. Well, it is very different on the passenger side in that we do a watchlist analysis on whether the passenger is on one of the watchlists. We do not do beyond that in terms of further background check or interview, particularly unless somebody presents a problem at the checkpoint. So there is a little bit of a dif-

ferent model. And we, as you know, do extensive physical security on passengers as they come through where more special attention is required.

Mr. BILIRAKIS. Okay. The bill that was approved in the subcommittee last week would increase from 100 to 500 the number of surface transportation security inspectors between now and 2010. What other areas might this committee consider supplementing to bolster rail and public transportation security?

Mr. HAWLEY. I think the committee has done—it is focus on the critical pieces, which are training. There is a lot in here that gets from the principle of training down to delivered training and the priority of delivered training. And I think that is absolutely right on in the surface arena, both for transit and in freight rail. So I think that is one. Information sharing is one.

You know, we have moved beyond the what are we going to do. I think we know what the critical pieces are with the fundamental pieces are. And now it is about the when are we going to do it and how quickly can we get it out there.

So things that accelerate the process by removing, you know, making the process streamlined, like in training. We have now got a system where we can turn it around in 90 days. You say I need so many people trained in this category. We can now turn that around right away. So those are the areas I would highlight.

Mr. BILIRAKIS. Okay, thank you.

Thank you, Mr. Chairman.

Mr. THOMPSON. Thank you very much.

I now yield to the gentleman from North Carolina, Mr. Etheridge.

Mr. ETHERIDGE. Thank you, Mr. Chairman. Let me thank you and the ranking member and the subcommittees for getting this bill before us.

Let me ask a question, Mr. Hawley, of you. According to the GAO and the FRA it has been focusing on efforts to improve rail safety. They have been addressing issues such as human error inspection and rail track failure. It seems, according to this report, or at least the report I have read, that—it says that the safety issue tends to be more pressing than the risk of terrorism.

My question to you is, if you will share with us, what is the synergy between safety and security concerns and where do these issues overlap when they do diverge. And secondly, what measures have been or can be implemented to serve both purposes of safety and security so you maximize the limited dollars that we have?

Mr. HAWLEY. Yes, sir, I appreciate the question. I think it is a critical point, particularly in freight rail where the things like the stability of the rail car and the integrity of the hull, particularly if something is carrying a dangerous chemical.

That very much has to do with safety, but it has a clear security need. And it highlights the necessary relationship between DHS and DOT so that we know what they are doing on the safety side and we can say this would have more of a security impact and so as that we do not use our resources to double the effort that they have already done. So we know what they are doing.

One example is inspectors where we now are cross-training inspectors for the Federal Rail Administration to look for security

type of things while they are out there anyway. And we focused our efforts on where we considered the vulnerability, which is a TIH car or the toxic inhalation hazard car sitting unattended. And that is where we get after it because it is not so much a safety issue, but that really is a security issue. So that is where we focus.

Mr. ETHERIDGE. So you are talking about open lines of communication?

Mr. HAWLEY. Very definitely.

Mr. ETHERIDGE. All right. Let me move to another one because part of the difficulty, I know, as we talk about mass transit of serving is really the open nature of the system, you know, the multiple access points, the large number of people that we serve on a very tight schedule at short periods of time and the need of passenger flow because of the amount of it. Research, I think, is needed into methods of attaining security without shutting down the system.

My question is this. I know there has been a few initiatives in the past such as TRIP, the pilot project in Maryland, et cetera. And there is a wealth of information, I think, that we can draw from from experiences from people like, well, Mr. Falkenrath, who is with us this morning can certainly share things in New York. But there is also experiences from other nations, and particularly Israel and others who have really done a lot to secure their system.

My question, Mr. Hawley, is what steps has the department taken to develop a robust research and development program for rail and mass transit security? And what lessons are being taken from the practices and technologies of other countries?

And then I hope, Mr. Falkenrath, you will have a moment to tell us what are your prognosis for the ability to develop and deploy a system that will actually offer this kind of security.

Mr. HAWLEY. Sure. We work very closely with other countries and in sharing information on screening, specifically with the U.K. I have had the opportunity to meet with them on some of their pilots in both transit and aviation that give us some interesting results. We do that pilot. You mentioned the ones, the TRIP and other ones that we have done.

We have established we can do screening. The issue is with so many people going through, it has to be on a segregated basis, either by random or based on behavior. So we look at explosive detection technology and behavior detection technology as the two best ways of figuring stand-off detection to select who might be the problem you do encounter. And then I know New York City is very aggressive on this.

Mr. FALKENRATH. Yes, we have a bag search program and an explosive detection program that is deployed every day in the subway. It was challenged in federal court. We were sued. The federal court upheld the legality of that. And after they did so, other jurisdictions began to adopt the practice like the state police of Massachusetts. So we have a lot of practice with this.

We do not do behavioral recognition. The officers who run this are told to pick people simply on the basis of numbers, every tenth or every twentieth person. And they are just pulled aside. But if someone changes their behavior when they see the screening patrol, like walks away, turns around, we will respond to that in addition.

I don't believe that this practice was learned from any other country. I believe it was pioneered in New York City. And we do it on our own nickel.

Mr. ETHERIDGE. Thank you. Let me thank all of you for your service and your commitment. This is a big issue. And any thoughts you have as this legislation moves that can make it better and more secure for this country, we would appreciate it.

Thank you, Mr. Chairman. I yield back.

Mr. THOMPSON. Thank you very much.

I now yield to the gentleman from California, Mr. Lungren.

Mr. LUNGREN. Thank you very much, Mr. Chairman. I appreciate it.

And I thank all of you for your service.

And I would say that I as the ranking member of the subcommittee from whence this bill came, I am proud of the bill with a couple of exceptions that I am concerned about. And for the gentleman from the Labor Department—and I understand there is some questioning that has already gone into this. But I would like to get down to this part.

Dealing with the whistle-blower section, this proposed legislation would require OSHA to investigate all whistle-blower claims resulting from, and I quote the bill, "an alleged violation of any law, rule or regulation relating to national or homeland security." Right now in looking at whistle-blower claims, does OSHA deal with intelligence and security matters?

Mr. FAIRFAX. No, not directly under the whistle-blower statutes.

Mr. LUNGREN. So you haven't developed an expertise in making judgments with respect to security, either homeland security or national security matters?

Mr. FAIRFAX. No.

Mr. LUNGREN. Or intelligence matters?

Mr. FAIRFAX. No, we haven't. I mean, when we have taken over other statutes on whistle-blower protection, we have been in the same situation, though, where we have had to, you know, work with the other respective agencies, train our people and move forward. But to answer your question, no, we don't have—

Mr. LUNGREN. No, I understand you work in other areas. But we are talking about national security and homeland security and intelligence, which at least we treat somewhat differently in the Congress because of the difference of its very nature.

Mr. FAIRFAX. Right.

Mr. LUNGREN. Mr. Falkenrath from the New York City Police Department, again, I want to talk about the whistle-blower protection provisions. These also would apply under this bill to state and local government employees of public transportation agency.

It provides for penalties for whistle-blower retaliation of up to 10 years imprisonment and up to $5 million in punitive damages. How would that affect local government employees? In other words, are you concerned that managers would be hesitant to remove employees that appear to present a security risk due to fear of criminal and civil liability?

And the bill also says that if the jurisdiction involved were to raise a state secret issue—that is, it involves intelligence—that automatically the ruling would be against the entity. In other

words, if you dared on any level of the government raise the fact that you could not disclose to the court the reason for the action taken based on intelligence, that that automatically would allow the claimant to win his or her lawsuit in terms of funds.

Mr. FALKENRATH. Sir, the provisions you describe sound troubling. But I apologize I am going to have to get you an answer for the record. We are going to need to study that exact provision and provide you the answer you seek in writing.

Mr. LUNGREN. And, Mr. Hawley, could you render an opinion on how that might impact your department or some of these other agencies with which you work?

Mr. HAWLEY. I would have to study the more detail on this particular provision. But obviously, as you point out, maintaining classified information is of paramount importance to the security mission. And there is the balance that says so is the ability of employees not to be improperly subject to retribution. So this has not been raised to me as a subject that we have had concern as we have looked at the bill. But I will look at it again with the perspective you raise.

Mr. LUNGREN. I mean, see, I understand the idea we want to balance it. But it sounds to me that tilts it in one fashion. When we are dealing with issues of homeland security and we say if the government dares raise the issue of sensitive intelligence, automatically the claimant wins, that may be the way some people think it ought to work.

But I just wonder whether we are serious about the threat that is out there and understand that intelligence is such a key aspect to our ability to defend ourselves. And that is not taking anything away from trying to protect workers against being unduly acted upon. But I just wish you would look at that and give us a response.

Thank you very much, Mr. Chairman.

Mr. THOMPSON. Thank you very much.

Just for the record, Mr. Fairfax, when you received the Sarbanes–Oxley responsibility for whistle-blower, how much expertise did labor have in financial?

Mr. FAIRFAX. Well, very little in OSHA. We brought people in to train our people. But we did not have expertise in that area.

Mr. THOMPSON. And so, you brought them all, and you have now developed—

Mr. FAIRFAX. We worked with the Securities and Exchange Commission. We brought in people from the Department of Justice to train our people. And then if need be, we contract out and bring in other experts to help with financial matters.

Mr. THOMPSON. So it is your testimony that you basically have created the expertise once you were given the responsibility?

Mr. FAIRFAX. Yes.

Mr. THOMPSON. Thank you.

I now yield to the gentleman from Texas, Mr. Cuellar.

Mr. CUELLAR. Thank you, Mr. Chairman. Thank you for your leadership on this bill that I support.

And again, gentlemen, thank you for being here with us.

I want to follow up on a line of questioning that Mr. Bilirakis just brought up about the border. I am from Laredo, the border

area, as you know. If you have a family that is sitting in the living room or the kitchen and they are worried about an outside threat, let us say, outside invasion, we certainly want to do everything to protect them in their living room and the kitchen. But at the same, we can't forget about the front door.

Just like the border is our front door to literally hundreds of thousands of rail cars coming in. For example, in the Laredo area, northbound and southbound in 2006 we had over 401,000 rail cars that came in. And keep in mind that we depend a lot on what happens in Mexico, that is the what is screened and what comes in and the contractors that are involved to get that work done.

Buses, for example, in the Laredo area—7and I am just giving you just a snapshot—we have over 100 buses that come a day. That is, people coming from Mexico coming in with no inspection station in place there and still 100 buses. And I believe in 2005 we had 35,841 separate buses that came in just through that part. And that doesn't include the 4 million trucks that come in, the containers. So I am just talking about the rail and the buses that are coming in.

Are we doing enough to protect ourselves for the rail cars coming in and the buses coming in from other countries? Any suggestions that you can give us? And I know this has to do more with Customs. And I don't know if you have any suggestions. Maybe we ought to make a minor modification on the international bridges that we have, international rail bridges that we have to cover some of this infrastructure and rails that are coming in from foreign countries. And in particular, I am talking about Mexico and the border, the Southwest border.

Mr. HAWLEY. I wouldn't have any legislative proposal. But as you point out, it is a shared responsibility. And the Customs and Border Protection has people on the ground there. We have an interest obviously and coordinate with them. And then we take responsibility as it moves inland into the United States.

And then I think on your second panel you will have another party. The railroad industry has a piece of that, too. So we all work together. But I think you have put your finger exactly on the issue. And it is what Mr. Langevin was talking to me about, of the things that we worry about is not being totally connected.

And I think we have become since 9/11 a whole lot more better connected. And we do recognize that it is the total journey, not just what started in Mexico but coming across the border or any border really and where it goes in the United States. It is one seamless thing. And we have to watch the whole piece.

Mr. CUELLAR. And do we have a seamless trail that we can follow right now?

Mr. HAWLEY. Well, information is the key. And that is why having the railroads in that because it is their customers and they track it and not at our expense. But we have the ability to reach in and find out what we need to know on an almost real time basis from railroads if we have a concern about either a category of goods or specific cars that we need to track anywhere as it is in the United States.

Mr. CUELLAR. Are we able to track the hazardous materials that are coming in through our—and again, I am not even talking about

the millions of trucks that we have on a yearly basis, but just the rail cars right now?

Mr. HAWLEY. In the United States we absolutely are. I don't know exactly what they get coming in advance of the border. But once it is in the United States, we have very granular ability to find cars, to know where they are.

Mr. CUELLAR. Once they cross the border, or once they get into our screen inside the United States?

Mr. HAWLEY. I am personally only familiar with once it is in the United States. I don't know exactly what we have prior to the border entry. I could get that from Customs and Border Protection and supply it for the record.

Mr. CUELLAR. Okay. All right. I would ask you if you have any other suggestions because, I mean, I am very supportive of this legislation. But I just want to make sure that we look at not only taking care of our families in the kitchens and in the living rooms, but making sure that our front door is well-protected.

Being from the border and having my family in the border I certainly want to make sure that we take care of the front door. Thank you.

I yield back the remainder of my time, Mr. Chairman.

Mr. THOMPSON. Thank you very much.

I now yield to the gentleman from Pennsylvania, Mr. Carney.

Mr. CARNEY. Thank you, Mr. Chairman. Thank you for your leadership on this bill. It is great.

This question is for Mr. Hawley and Mr. Rosapep. In 2005, the GAO testified before the Senate Committee on Commerce, Science and Transportation that coordination between the Departments of Homeland Security and Transportation could be improved, noting that the lack of coordination could lead to confusion, duplication, and gaps in preparedness. Has coordination improved?

Mr. HAWLEY. Yes. And since that time, we have arranged a memorandum of understanding. And we have charted it out. And we have both formal and informal communications. And frankly, I think we rely on each other moving forward. And it is a very tight, I think, very positive relationship.

Mr. CARNEY. So the gaps are closed or closing?

Mr. HAWLEY. I believe so, yes.

Mr. ROSAPEP. I would agree. I mean, since we have adopted the MOU we really have stood up a structure for staff to be working. We have an executive steering committee to coordinate the overall security and transit security efforts. We have eight working groups that have staff from both agencies involved to address all the important elements really that are in your bill. And we have a group on training. We have a group on grants, a group on standards and so forth.

So there really is the structure in place to provide that coordination. It is a work in progress, but the structure really is there.

Mr. CARNEY. It is an iterative process, you would say?

Mr. ROSAPEP. Yes, I mean, to be honest, I mean, all this is about relationships between people. And as you are working closer together, you start to learn each other's strengths and weaknesses and how to complement each other.

Mr. HAWLEY. I think it is only fair to point out that as we have made tremendous progress certainly with DHS and DOT that—talk about personal relationships, you know, Commissioner Falkenrath, you know, I feel good communications there. But that would be an area where we really need to take the next step, is to get those closer connections certainly with TSA to be better connected to our operating partners at the local level. And that is really the primary focus of our activity now, is to close those gaps.

Mr. CARNEY. What steps would you recommend that we take, formal or informal, for that matter, to make that happen?

Mr. HAWLEY. Well, I think a lot of it gets down to the basics of communication. And I would like Commissioner Falkenrath to offer his perspective. He certainly has been very clear to me in expressing it and should share it with the committee. But it starts with who do I call. You know, it is DHS. You know, where is my point of contact that can track getting information flowing both ways? And for an organization as sophisticated and as real time as NYPD, you know, that is a moving part, as are we. So that, I think, is the challenge.

Mr. FALKENRATH. It is not complicated. You pick up the phone. You call. You say we need to work on this together, and we want to do it. If you are having a meeting, you invite the agencies that are involved. You do not rely solely on the agencies you have worked with historically. You take a look at where the risk is and you figure out which agencies are critical for addressing that risk on a day to day basis. And you bring them in front and center.

Mr. CARNEY. I agree. I mean, it is not all—the obvious things are not always the things we do. And I am glad to see some common sense is prevailing here. Those sorts of relationships are absolutely critical, not only to the day to day operation, but to build in the culture of cooperation.

And I think that is where, from my perspective at least, DHS has been woefully deficient, is creating the culture. And I think this is a step toward that. And I think we are going to be—you know, we are certainly heading in the right direction. I appreciate your comments. Thank you.

Mr. THOMPSON. Thank you very much.

Let me say how much we appreciate the first panel for their presentation and how you responded to all the questions from the members. Thank you very much.

We will now take a short break until we can get set up for the second panel.

I welcome the second panel of witnesses.

Bill Millar is the president of the American Public Transit Association, which represents public transportation systems across the nation.

Ed Hamberger is the president of the American Association of Railroads.

Ed Rodzwicz is the president of the Teamsters Rail Conference, which represents thousands of frontline rail and public transportation workers.

Fred Weiderhold is the inspector general of Amtrak.

And I guess Mr. Shuman is on his way, who is an independent transportation consultant with nearly 30 years of experience assisting railroads.

Without objection, the witnesses' full statement will be inserted in the record.

And because of time constraints, I would ask each witness to try to summarize his statement for about 3 minutes or the best you can do, beginning with Mr. Millar. And I know that is tough for this bunch.

STATEMENT BILL MILLAR, PRESIDENT, AMERICAN PUBLIC TRANSPORTATION ASSOCIATION

Mr. MILLAR. Yes, sir. Thank you, Mr. Chairman. And on behalf of the 1,500 members of the American Public Transportation Association, I am pleased to be here today and to give you our views on the proposed Rail and Public Transportation Security Act of 2007.

I want to start by particularly thanking you, Mr. Chairman, for your long support of improving security for public transportation. And we look forward to continuing to work with you and the committee in that regard.

On an annual basis, over 10 billion times Americans used public transportation, less than 1 billion times that they used the nation's airline system. Unfortunately, security has been an issue for our industry for a long time.

According to the Government Accountability Office, about one-third of terrorists' attacks worldwide target transportation systems and transit systems are the mode most commonly attacked. U.S. transit systems have worked with our customers to protect their customers against terrorism since long before September 11, 2001. But certainly, since 9/11, we, like everyone else in our society, has stepped up our concern about this.

Our industry so far has spent more than $2.5 billion of its own money in addition to a small amount of federal assistance that has been provided for security. Overall, we have identified over $6 billion worth of security investments that should be made. Some of these are simple.

Some are complex, things like interoperable communications systems, greater use of security cameras, automated vehicle locator systems, and a variety of other capital expenditures. But also investment is needed in so-called soft costs such as law enforcement personnel, overtime costs for transit employees, extra security, more extensive worker training, and a whole host of other costs that we face.

We would ask the Congress also to provide funding to sustain APTA's security standards program, which is an ongoing effort in cooperation with DHS and DOT. We would also urge—and I know Ms. Harman commented on this earlier. We would urge Congress to provide funding to maintain the public transit information sharing and analysis center, the so-called ISAC, which is the link that brings that world of intelligence to public transportation that is so important.

Turning to the specifics of the Rail and Public Transportation Security Act, we strongly support the $3.36 billion which would be

authorized for security grants under this bill. These investments would enable us to make a considerable dent in the $6 billion worth of needs. And we are very appreciative that these funds would be available for operational and capital needs.

We do encourage the Congress to recognize and provide flexibility as needs from city to city, locality to locality very substantially. Large rail systems are different than smaller bus systems. Both are different than commuter rail.

We do have some concerns about the bill's details and how these details might be implemented by the Department of Homeland Security. We are concerned that they have created a complicated and inefficient grants distribution process. And we have ideas to improve that process.

We are concerned about the requirement for a local match. We wonder what 600 rail inspectors, many of whom do not understand the public transit operating environment, will do. We worry about the negative impact of the threat of civil and criminal penalties.

And we are concerned that grant funds appropriated would not be delivered expeditiously. We believe that if there were cooperation with the Federal Transmit Administration its well-established grant delivery program could be used, even if the policy is set by the Congress and the DHS, which we completely agree with in terms of security.

We fully support security training. But training requires funds, not only for the training itself, but in our business, if an employee is away from driving a bus, let us say, to get properly trained, there is nobody to drive the bus. So we have to make sure that there is money there to provide substitutes so that our staff members can have proper and appropriate amounts of training without denigrating service to our riders, without increasing transit fares and without raising local taxes.

We would hope that the legislation could provide for the ISAC, as I mentioned earlier. And finally, we support the concept of coordination of transportation security tools and resources through a national center of excellence. Within that concept, we would recommend that organizations already federally funded such as the National Transit Institute at Rutgers or the Mineta Institute at San Jose State University ought to be key elements to that.

Mr. Chairman, again, I want to thank you for your leadership and the leadership on this committee in this effort. This is a national issue that must have a national response. We look forward to working with you as you craft the details of your proposal.

Thank you very much.

[The statement of Mr. Millar follows:]

PREPARED STATEMENT OF WILLIAM W. MILLAR

Mr. Chairman, thank you for this opportunity to provide testimony to the Committee on the Rail and Public Transportation Security Act of 2007. We appreciate your making the security of the tens of millions of Americans who use public transportation an important priority of this Committee, and we look forward to working with you on this issue. We thank you for your leadership on transit security.

ABOUT APTA

The American Public Transportation Association (APTA) is a nonprofit international association of more than 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. APTA members serve the public interest by providing safe, efficient, and economical transit services and products. More than ninety percent of the people using public transportation in the United States and Canada are served by APTA member systems.

OVERVIEW

Mr. Chairman, public transportation is one of the nation's critical infrastructures. We cannot overemphasize the critical importance of the service we provide in communities throughout the country. Americans take about 10 billion transit trips each year. People use public transportation vehicles over 34 million times each weekday. This is more than eighteen times the number of daily domestic boardings on the nation's airlines.

Safety and security are the top priority of the public transportation industry. The Government Accountability Office (GAO) released a report several years ago which said "about one-third of terrorist attacks worldwide target transportation systems, and transit systems are the mode most commonly attacked." Transit agencies had already taken many steps to improve security prior to the September 11, 2001 terrorist attacks and have significantly increased efforts since that date. Since 9/11, public transit agencies in the United States have spent over $2.5 billion on security and emergency preparedness programs, and technology to support those programs, largely from their own budgets with only minimal federal funding.

Since 9/11, the federal government has spent over $24 billion on aviation security while has only allocated $549 million for transit security. Last year's attacks in Mumbai and the previous attacks in London and Madrid further highlight the need to strengthen security on public transit agencies in the U.S. and to do so without delay. We need to do what we can to prevent the kind of attacks that caused more than 400 deaths and nearly 3,000 injuries on rail systems in Mumbai, London and Madrid.

We urge Congress to act decisively. While transit agencies are doing their part, we need the federal government to be a full partner in the fight against terrorism. Terrorist attacks against U.S. citizens are clearly a federal responsibility and the federal government needs to increase its support for transit security improvements. In light of documented needs, we urge Congress to increase federal support for transit security grants to assist transit agencies in addressing the $6 billion in identified security needs. We ask that Congress provide no less than $545 million in the Fiscal Year (FY) 2008 Homeland Security Appropriations bill for transit security. Funding at that level annually would allow for significant security improvements in the nation's transit agencies over a 10-year period. Federal funding for additional security needs should provide for both hard and soft costs as described below and be separate from investments in the federal transit capital program.

We also urge Congress to provide $500,000 to the Department of Homeland Security (DHS) for grant funding to the APTA security standards program, under which APTA is working with its federal partners to develop transit security standards. Finally, we urge Congress to provide $600,000 annually to maintain the Public Transit Information Sharing Analysis Center (ISAC) which provides for the sharing of security information between transit agencies and DHS.

To improve the distribution of funds under the existing transit security programs, we recommend that the existing process for distributing DHS grants be modified so that grants are made directly to transit agencies, rather than through State Administrating Agencies (SAA). We believe direct funding to transit agencies would be quicker and cheaper. The current process and grant approval procedures have created significant barriers and time delays in getting funds into the hands of transit agencies for security improvements. We believe that DHS should work with Federal Transit Administration (FTA) on the distribution of funds since FTA understands transit and already effectively administers a much larger capital grant program to transit agencies.

As transit security is part of the larger war on terrorism, we urge Congress to continue providing transit security grants with no state or local match requirement. A local or state match requirement would have detrimental consequences by making security improvements contingent on a community's ability to raise local funding. A local match requires the approval of a local governing body. Approval of such grants in an open, public forum, where specific project information is discussed is simply inappropriate for security sensitive projects. We should not make such information available to potential terrorists.

BACKGROUND

In 2004, APTA surveyed its U.S. transit agency members to determine what actions were needed to improve security for their customers, employees and facilities. In response to the survey, transit agencies around the country identified in excess of $6 billion in transit security investment needs.

In FY 2003, $65 million in federal funds were allocated by DHS for 20 transit agencies. In FY 2004, $50 million was allocated by DHS for 30 transit agencies. In FY 2005, Congress specifically appropriated $150 million for transit, passenger and freight rail security. Out of the $150 million, transit received $135 million. In FY 2006, Congress appropriated $150 million. Out of the $150 million, transit received $136 million. In FY 2007, Congress appropriated $175 million. Out of $175 million, transit is slated to receive $163 million. We appreciate these efforts, but more needs to be done.

Transit agencies have significant and specific transit security needs. Based on APTA's 2003 Infrastructure Database survey, over 2,000 rail stations have no security cameras. According to our 2005 Transit Vehicle Database, 53,000 buses, over 5,000 commuter rail cars, and over 10,000 heavy rail cars have no security cameras. Less than one-half of all buses have automatic vehicle locator systems (AVLs) that allow dispatchers to know the location of the bus if an emergency occurs. Nearly seventy-five percent of demand response vehicles lack these AVLs. Furthermore, no transit agency has a permanent biological detection system. In addition, only two transit agencies have a permanent chemical detection system. A more robust partnership with the federal government would help to better address many of these specific needs.

We are disappointed that the Administration proposed only $175 million for transit, passenger and freight rail security in the FY 2008 DHS budget proposal. Regrettably, the Administration failed to make a significant funding proposal to enhance the security of the tens of millions of Americans who use transit. Instead, the Administration chose to freeze security funding for transit, passenger rail, and freight rail security at the level in FY 2007. This funding level falls well short of the funds needed to ensure the safety of Americans who take public transportation. We are also disappointed that the Administration failed to propose funding for transit security standards or the Public Transit ISAC. Both of these programs could significantly enhance transit security for a minimal cost.

APTA is a Standards Development Organization (SDO) for the public transportation industry. We are now applying our growing expertise in standards development to transit industry safety and security, best practices, guidelines and standards. We have already initiated our efforts for security standards development and have engaged our federal partners from both the DHS and DOT in support of this initiative. Unfortunately, DHS has not agreed to provide funding to APTA for this effort. We respectfully urge Congress to provide $500,000 to the DHS so that it can provide that amount in grant funding to the APTA security standards program. Our efforts in standards development for commuter rail, rail transit and bus transit operations have been significant and our status as a SDO is acknowledged by both the FTA and the Federal Railroad Administration (FRA). The FTA and the Transportation Research Board have supported our standards initiatives through the provision of grants while our members have dedicated a portion of their APTA dues for standards development.

We also would like to work with Congress and the Department of Homeland Security's Directorate of Science and Technology to take a leadership role in advancing research and technology development to enhance security and emergency preparedness for public transportation.

SECURITY GRANT PROGRAM

The DHS's Office of Grants and Training (G&T) is responsible for the distribution of the transit security grant program. G&T should be commended for reaching out to the transit industry in numerous listening sessions on our concerns. Staff from G&T have attended APTA conferences and participated in panel discussions. G&T staff has conducted various conferences around the country to explain the details of the transit security grant program. We continue to work with G&T on streamlining and improving the grant program but are frustrated with the results thus far.

Since the creation of the DHS, four separate offices have been responsible for the distribution of transit security grants. Funds were originally distributed by the Office for Domestic Preparedness (ODP). Then it became known as the Office of State and Local Government Coordination and Preparedness (SLGCP). Now it is known as the Office of Grants and Training (G&T). In addition, the Transportation Security Administration (TSA) is responsible for establishing policy for the program and must now coordinate with G&T.

Along with the organizational changes, each new office has changed the distribution process for the transit security grants. In FY 2003 under ODP, grants went directly to the transit authorities. In FY 2004 under SLGCP, grants went to the State Administrating Agencies (SAAs), which then distributed grants to the transit systems. In FY 2005 under SLGCP, grants went through the SAAs, which then distributed grants to eligible transit systems on a regional basis in coordination with the urban area. Eligible transit systems were then required to work with the SAAs, the urban area, and the other eligible transit systems in their region to come up with a regional transit security plan on how to spend the federal funding before the transit system could be awarded the grant. This is currently the process.

The transit systems that have been allocated DHS funds are accustomed to receiving federal transit funding directly to designated recipients from the FTA under authorizing law. We believe that DHS should work with the FTA in distributing grants to take advantage of FTA's current familiarity with transit agencies and its own grant making process. While we believe Congress should continue to make federal transit security grants available through the DHS, the FTA model has been in place for years and works well in distributing funds quickly to transit systems. In contrast, DHS's current process and conditions have created significant barriers and time delays in getting funds into the hands of transit agencies where they can be used to protect riders. We urge Congress to get transit security grants directly to the transit authorities in a way that takes advantage of FTA's experience and effective delivery system.

In that regard, we note that Section 3028, Subsection (c) of Safe, Accountable, Flexible, Efficient Transportation Equity Act—A Legacy for Users, SAFETEA–LU (P.L. 109–59) requires the Secretary of Transportation and the Secretary of the Department of Homeland Security to "issue jointly final regulations to establish the characteristics of and requirements for public transportation security grants, including funding priorities, eligible activities, methods for awarding grants, and limitations on administrative expenses." We believe this rulemaking could be used to address our concerns and we ask the Committee to direct that it do so.

INFORMATION SHARING

Since the terrorist attacks of September 11, 2001, public transit agencies across the country have worked diligently to strengthen their security plans and procedures. They have also been very active in training personnel and conducting drills to test their capacity to respond to emergencies. Also, to the extent possible within their respective budgets, transit agencies have been incrementally hardening their facilities through the introduction of technologies such as surveillance equipment, access control and intrusion detection systems. While transit agencies have been diligent, they have been unable to fully implement programs with current levels of assistance from the federal government.

A vital component of ensuring public transit's ability to prepare and respond to critical events is timely receipt of security intelligence in the form of threats, warnings, advisories and access to informational resources. Accordingly, in 2003, the American Public Transportation Association, supported by Presidential Decision Directive #63, established an ISAC for public transit agencies throughout the United States. A grant in the amount of $1.2 million was awarded to APTA by the Federal Transit Administration to establish and operate a very successful Public Transit ISAC that operated 24 hours a day, 7 days a week, and gathered information from various sources, including DHS. The ISAC also passed information on to transit agencies following a careful analysis of that information. However, given that the Federal Transit Administration was subsequently unable to access security funds, and given the decision of DHS to not fund ISAC operations, APTA has had to look for an alternate method of providing security intelligence through DHS's newly created Homeland Security Information Network (HSIN). APTA continues to work with DHS staff to create a useful HSIN application for the transit industry. It is clear, however, that while the HSIN may become an effective resource, it does not duplicate or provide the 24/7 two-way communication functions provided through the Public Transit ISAC. We believe that consistent, on-going and reliable funds from Congress should be provided for the Public Transit ISAC which has been proven an effective delivery mechanism for security intelligence. We respectfully urge Congress to provide $600,000 annually to maintain the Public Transit ISAC.

In addition, APTA's membership includes many major international public transportation systems, including the London Underground, Madrid Metro, and the Moscow Metro. APTA also has a strong partnership with the European-based transportation association, the International Union of Public Transport. Through these relationships, APTA has participated in a number of special forums in Europe and Asia

to give U.S. transit agencies the benefit of their experiences and to help address transit security both here and abroad.

COST OF HEIGHTENED SECURITY

Following the attacks in London in 2005, APTA was asked to assist the Transportation Security Administration (TSA) in conducting a teleconference between the TSA and transit officials to discuss transit impacts pertaining to both increasing and decreasing the DHS threat levels. There is no question that increased threat levels have a dramatic impact on budget expenditures of transit agencies and extended periods pose significant impacts on personnel costs. The costs totaled $900,000 per day for U.S. public transit agencies or an estimated $33.3 million from July 7 to August 12, 2005 during the heightened state of "orange" for public transportation. This amount does not include costs associated with additional efforts by New York, New Jersey and other systems to conduct random searches.

Many transit agencies are also implementing other major programs to upgrade security. For example, New York's Metropolitan Transportation Authority (NY–MTA) is taking broad and sweeping steps to help ensure the safety and security of its transportation systems in what are among the most extensive security measures taken by a public transportation system to date. NY-MTA will add 1,000 surveillance cameras and 3,000 motion sensors to its network of subways and commuter rail facilities as part of a $260 million Integrated Electronic Security System. In fact, NY–MTA plans to spend over $1.2 billion on transit security.

SECURITY INVESTMENT NEEDS

Mr. Chairman, since the awful events of 9/11, the transit agencies have invested more than $2.5 billion of their own funds for enhanced security measures, building on the industry's already considerable efforts. At the same time, our industry undertook a comprehensive review to determine how we could build upon our existing industry security practices. This included a range of activities, which include research, best practices, education, information sharing in the industry, and surveys. As a result of these efforts we have a better understanding of how to create a more secure environment for our riders and the most critical security investment needs.

Our survey of public transportation security identified enhancements of at least $5.2 billion in additional capital funding to maintain, modernize, and expand transit system security functions to meet increased security demands. Over $800 million in increased costs for security personnel, training, technical support, and research and development have been identified, bringing total additional transit security funding needs to more than $6 billion.

Responding transit agencies were asked to prioritize the uses for which they required additional federal investment for security improvements. Priority examples of operational improvements include:

- Funding current and additional transit agency and local law enforcement personnel
- Funding for over-time costs and extra security personnel during heightened alert levels
- Training for security personnel
- Joint transit/law enforcement training
- Security planning activities
- Security training for other transit personnel

Priority examples of security capital investment improvements include:

- Radio communications systems
- Security cameras on-board transit vehicles and in transit stations
- Controlling access to transit facilities and secure areas
- Automated vehicle locator systems
- Security fencing around facilities

Transit agencies with large rail operations also reported a priority need for federal capital funding for intrusion detection devices.

ONGOING TRANSIT SECURITY PROGRAMS

Mr. Chairman, while transit agencies have moved to a heightened level of security alertness, the leadership of APTA has been actively working with its strategic partners to develop a practical plan to address our industry's security and emergency preparedness needs. In light of our new realities for security, the APTA Executive Committee has established a Security Affairs Steering Committee. This committee

addresses our security strategic issues and directions for our initiatives. This committee will also serve as the mass transit sector coordination council that will interface with DHS and other federal agencies forming the government coordinating council.

In partnerships with the Transportation Research Board, APTA supported two TCRP panels that identified and initiated specific projects developed to address *Preparedness/Detection/Response to Incidents and Prevention and Mitigation.*

In addition to the TCRP funded efforts, APTA has been instrumental in the development of numerous security and emergency preparedness tools and resources. Many of these resources were developed in close partnership with the FTA and we are presently focused on continuing that same level of partnership with various entities within DHS. Also, APTA has reached out to other organizations and international transportation associations to formally engage in sharing information on our respective security programs and to continue efforts that raise the bar for safety and security effectiveness.

RAIL AND PUBLIC TRANSPORTATION SECURITY ACT OF 2007

Mr. Chairman, we thank you for making public transportation security improvements a priority for your Committee. We appreciate your interest and support for strengthening the federal program intended to protect tens of millions of transit users and the hundreds of thousands of transit workers against terrorism. We appreciate the $3.36 billion which would be authorized for transit security grants under this bill and believe it would allow us to make considerable progress in addressing the $6 billion in transit security needs that have been identified.

This legislation and current programs place the responsibility for transit security squarely on the DHS, however we urge the Congress to require DHS to effectively partner with both transit agencies and the FTA in its efforts to enhance transit security. Every major transit agency has already conducted security risk assessments for their system. Transit agency operators understand their security vulnerabilities and needs. While we understand the need for DHS and the Congress to ensure that limited resources are used as efficiently as possible, we also feel strongly that providing these systems with the resources to deter, detect, and prevent terrorist activities, and to respond effectively if a critical event does occur, should be of paramount importance. We remain convinced that a more efficient delivery system for grants, ideally one where funds go directly to transit agencies, is one of the most effective ways to enhance security. The current system where agencies, after receiving an allocation, must develop regional plans for use of grant funds, pass those proposals back up to DHS through state agencies, then have DHS often request grant proposal modifications which are passed back down through the chain before they are resubmitted and ultimately awarded has not worked well. It is slow and inefficient.

We also appreciate that funds under this bill are made available to address both operational and capital needs. Funding is needed to support additional security personnel, as well as overtime and salary costs related to training, drills, planning and risk assessments. Funding is also needed for technology and capital improvements. In both cases, however, we urge Congress to provide flexibility because assessments, technology, and operating needs do vary in different cities and among transit agencies with a wide variety of different operating conditions. Large rail systems are different from bus systems in smaller communities, and both are different than commuter rail operations. We believe that the determination of appropriate technology needs and operating improvements are something that is best done in partnership with the transit industry and not determined unilaterally by DHS. Further, the requirement for assessments at all agencies in communities with more than 50,000 people should recognize the differences among resources, capabilities and risks in different size communities and agencies.

We are also concerned about how the regulatory responsibility placed on DHS in the bill may move accountability away from the transit agencies themselves. Transit agencies should be held accountable for the efficient use of grant funds, but grant oversight should not become an impediment to using these grants to improve security. We also question whether the civil penalties and enforcement of regulations required under the bill will improve security. Transit systems are generally state, county, or municipal agencies headed by local officials responsible to the people of their community. If transit systems are fined, such penalties will essentially be paid by taxpayers and fare paying customers or come at the expense of transit service or transit security.

As noted earlier, we are concerned about the requirement for a state or local match for security grants. National security is a federal responsibility. Security should not be predicated on a community's ability to raise local tax funds. We are

also concerned about a process that would necessitate the detailed disclosure of how security funds are to be used in a public forum. A local match requires the approval of a local governing body. Approval of such grants in an open, public forum, where specific project information is discussed is simply inappropriate for security sensitive projects. We should not make such information available to potential terrorists.

We further urge Congress to fund the development of security standards and protocols by the industry, and for the Public Transit Information Sharing Analysis Center (ISAC). Security standards are currently being developed by APTA in partnership with DHS and the DOT, but, to date, funding support has not been provided by DHS. Similarly, the public transit ISAC continues to provide a vital 24/7 security information service to the transit industry and its continuation is also in need of funding support.

CONCLUSION

Mr. Chairman, I want to thank you for your leadership and to thank this Committee for its efforts to improve security in the nation's transit agencies. We pledge our cooperation as you continue to develop the national response to this issue. We genuinely appreciate the opportunity to comment on this important legislation and stand ready to work with DHS and the Congress to protect our riders, employees and communities against potential terrorist acts.

Mr. THOMPSON. Thank you very much, Mr. Millar.

Mr. Hamberger?

STATEMENT OF EDWARD HAMBERGER, PRESIDENT AMERICAN ASSOCIATION OF RAILROADS

Mr. HAMBERGER. Thank you, Mr. Chairman.

And just as Mr. Millar and I cooperated here this morning sharing a microphone, I would draw attention before the committee that every year close to half a billion of his passengers ride on freight rail right-of-way on commuter rails. So we cooperate out in the real world as well.

Thank you for the opportunity to discuss freight rail security in general and the Rail and Public Transportation Security Act of 2007 in particular. At your request, I will skip the general comments and get right into our views on some of the provisions in the bill.

First, I want to thank the subcommittee for its appreciation of the unique characteristics of the transportation technology center in Pueblo, Colorado. We strongly support the provision that would make TTCI a member of the National Domestic Preparedness Consortium. Today a facility specifically targeted out of the emergency response training for freight and passenger railroad environments is notably absent from the NDPC. Your legislation now corrects that oversight.

We also strongly support the provision calling on DHS to establish a research and development program for projects related to rail security. My written statement identifies a number of projects that we believe would significantly enhance rail security.

The rail industry recognizes the importance of whistle-blower protection for its employees. And, in fact, our employees already receive such protection under the Federal Railroad Safety Act. Creating a new separate system under the Department of Labor is duplicative and potentially confusing. Perhaps a better approach would be to expand the current whistle-blower protections to include security matters so that there are not two parallel systems. And I would respectfully ask you to take a look at that.

Turning to the issue of security training for railroad employees, it is an issue we take very seriously. And, in fact, working with the National Transit Institute at Rutgers University, referenced by Mr. Millar, freight railroads have developed an interactive uniform security awareness curriculum for freight rail employees. We submitted this training regimen to both TSA and the Federal Railroad Administration in 2006 and have received positive responses in return.

Recently TSA inspectors surveyed 2,600 railroad employees and found that 80 percent of those had a medium or high level of security awareness. All frontline class one rail employees will have completed this security training by the end of this year.

Finally, I would like to address the issue of background checks. I believe everyone understands the need for background checks. But it is imperative that that process be fair.

And I would like to thank this committee for bringing to the freight railroad industry's attention concerns with the background check for employees of railroad contractors. To help alleviate that confusion, as I testified 2 weeks ago, class one railroads have agreed to adopt new practices that include a robust appeals process, which will apply to individuals employed by railroad contractors who have been denied access to railroad property.

Under this process, not only the contractor, but the contract employee also will have the right to appeal the initial decision of access. And the employee will be so notified by the e-rail safe program. The appeals process will provide the contractor and the contractor employee an opportunity to supply additional information pertinent to the appeal, mitigating circumstances, for example. Once received, the appeal will be considered promptly by a diversified appeals board.

The provision adopted by the subcommittee in last week's markup does not seem to take into account the robust nature of this new voluntary system that the industry has set up. In addition, the adopted provision does not explicitly recognize that railroads have a broader need than security when doing background checks. These include workplace safety, drug, and alcohol abuse and protection of the property entrusted to us by our customers. I do appreciate commitments from staff to continue to work with us to try to clarify that particular facet of the amendment.

Finally, the adopted provision covers all rail employees, not just employees of rail contractors. There is already a grievance process in place for railroad employees, which has been arrived at through collective bargaining, includes union representation, and provides recourse and due process for our employees. So I respectfully suggest that the amendment does not need to extend to railroad employees.

We are proud of our security record since September 11th. And we look forward to continuing to work with this committee, our employees and other agencies as you go about your business of writing this legislation.

Thank you for the opportunity to be here.

[The statement of Mr. Hamberger follows:]

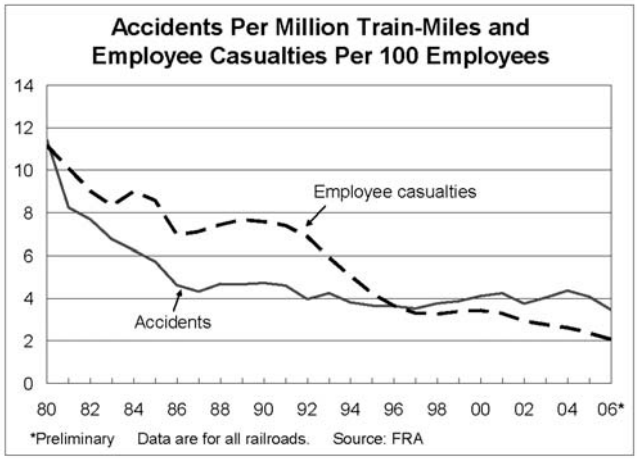
PREPARED STATEMENT OF EDWARD R. HAMBERGER

On behalf of the members of the Association of American Railroads (AAR), thank you for the opportunity to discuss freight railroad security in general and the Rail and Public Transportation Security Act of 2007 in particular. AAR members account for the vast majority of rail mileage, employees, and revenue in Canada, Mexico, and the United States.

Unlike U.S. passenger railroads and transit systems, U.S. freight railroads are, with minor exceptions, privately owned and operated, and they rely almost exclusively on their own earnings to fund their operations. Freight railroads move approximately 40 percent of our nation's freight (measured in ton-miles)—everything from lumber to vegetables, coal to orange juice, grain to automobiles, and chemicals to scrap iron—and connect businesses with each other across the country and with markets overseas.

From 1980 through 2006, Class I railroads spent more than $370 billion—more than 40 cents out of every revenue dollar—on capital expenditures and maintenance expenses related to infrastructure and equipment. Non-Class I carriers had billions of dollars of additional spending. These massive, privately-funded expenditures help ensure that railroads can meet our current and future freight transportation demands safely and cost effectively.

As the Federal Railroad Administration (FRA) noted in congressional testimony a few weeks ago, "The railroads have an outstanding record in moving all goods safely." Indeed, nothing is more important for railroads than the safety and security of their operations. For railroads, safety and security are interconnected: a safer workplace will tend to be a more secure workplace, and a more secure workplace will tend to be a safer workplace. And railroads have become much safer. According to FRA data, railroads reduced their overall train accident rate by 70 percent from 1980—2006, and their rate of employee casualties by 81 percent. Railroads have lower employee injury rates than other modes of transportation and most other major industry groups, including agriculture, construction, manufacturing, and private industry as a whole.



We should also be encouraged by the continuing improvements in rail safety. Based on preliminary data, 2006 was the safest year ever for railroads by the three most commonly-cited rail safety measures: the train accident rate, the employee casualty rate, and the grade crossing collision rate all reached record lows.

Freight railroads are justifiably proud of these accomplishments. At the same time, though, railroads want rail safety and security to continue to improve, and they are always willing to work cooperatively with members of this committee, others in Congress, the Department of Homeland Security (DHS), the Department of Transportation (DOT), the FRA, rail employees, and others to find practical, effective ways to make this happen.

To that end, we appreciate this committee's interest in rail security. Below I will describe the many ways that U.S. freight railroads have addressed security in the

post 9–11 era, provide our views on various provisions of the Rail and Public Transportation Security Act of 2007, and offer suggestions on how rail security can be further improved.

The Aftermath of September 11

Almost immediately after the 9/11 attacks, the AAR Board of Directors established a Railroad Security Task Force. The overarching goals of this task force were to (1) help ensure the safety of rail employees and the communities in which railroads operate; (2) protect the viability of national and regional economic activity; and (3) ensure that railroads can continue to play their vital role in support of our military.

Over the next several months, the task force conducted a comprehensive risk analysis of the freight rail industry. Using 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. Separate critical action teams covered information technology and communications; physical infrastructure; operational security; hazardous materials; and military traffic needs. Freight railroads also cooperated fully with a separate team covering passenger rail security.

The end result of these analyses was the creation of the industry's Terrorism Risk Analysis and Security Management Plan, a comprehensive, intelligence-driven, priority-based blueprint of actions designed to enhance freight railroad security. The plan was adopted by the AAR in December 2001 and remains in effect today.

As a result of the plan, freight railroads quickly enacted more than 50 permanent security-enhancing countermeasures. For example, access to key rail facilities and information has been restricted, and cyber-security procedures and techniques have been strengthened. In addition, the plan defines four progressively higher security alert levels and details a series of actions to be taken at each level:

Alert Level 1 is "New Normal Day-to-Day Operations." It 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 unauthorized persons to trace certain sensitive materials; and periodically confirming that security systems are working as intended.

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

Alert Level 3 means there is "a credible threat of an attack on the United States or railroad industry." 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 contractor 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, if intelligence has identified that terrorist action against a specific location or operation is imminent, for a particular geographic area (*e.g.,* the Midwest) or subset of rail traffic (*e.g.,* hazardous materials).

The rail security plan is not simply something that has been put in a binder on a shelf to be taken down and dusted off once in a while. Rather, it is a robust and dynamic paradigm for railroad operations that has been in effect for more than five years; it is evaluated and modified, as necessary, on an ongoing basis; and it has substantially raised the baseline of railroad security. Railroads took this action without waiting for legislation or a regulatory regime to tell them to do so.

Indeed, railroads are a model for other industries in their approach to improving security. As a former FRA administrator noted regarding rail efforts at enhancing security, "I can say how impressed I am by the scope of the analysis, the sophistication of the analytical framework, and the manner in which rail carriers have devoted substantial resources—both funding and senior leadership—to the completion

of this important task. They've done remarkable work." And a former Secretary of the U.S. Department of Health and Human Services has noted that "The anti-terrorist measures the railway industry has taken. . .have added and will continue to add to the safety of our citizens, the delivery of vital goods and the ability of our men and women in uniform to carry our battle to the enemy."

Access to pertinent intelligence information is a critical element of the railroad security plan. Congress should ensure that DHS is routinely communicating relevant intelligence to the railroad industry through the Railway Alert Network (RAN), a secure 24/7 communications network operated by the AAR at the Secret level that links federal security personnel with railroad operations centers. Through the RAN, railroads and the intelligence community can share information to maintain situational awareness and immediately institute appropriate alert levels.

Railroad industry security requires constant communication with the Transportation Security Administration (TSA) and elsewhere within DHS, the Department of Defense (DOD), the DOT, the FBI's National Joint Terrorism Task Force (NJTTF), state and local law enforcement, and others. A railroad police officer and railroad analysts who hold Top Secret clearances work with government intelligence analysts at NJTTF and at DHS to help evaluate intelligence and serve as subject matter experts.

Communication is also enhanced by the Surface Transportation Information Sharing and Analysis Center (ST–ISAC), which was established by the AAR at the request of the DOT. The ST–ISAC collects, analyzes, and distributes security information from worldwide resources to help protect vital information technology systems and physical assets from attack. It operates 24/7 at the Top Secret level.

Rail security efforts strongly benefit from the fact that major railroads have their own police forces. Safety and security would be enhanced if police officers of one railroad were permitted to exercise law enforcement powers on the property of another railroad. This flexibility could prove especially valuable in the event of a national security threat involving an individual railroad.

Notwithstanding rail industry efforts, there can be no 100 percent guarantee against terrorist assaults, including assaults involving hazardous materials (hazmat) on railroads. If such an incident occurs, railroads have well-established programs and procedures that would be invoked that are designed to respond to and minimize the impact of such incidents.

In this regard, emergency response efforts are critical. Railroads help communities develop and evaluate hazmat emergency response plans. Through their own efforts and the Transportation Community Awareness and Emergency Response Program (TRANSCAER), they provide basic training for more than 20,000 emergency responders each year.

In addition, more than 20 years ago, the AAR established the Emergency Response Training Center (ERTC), a world-class training facility that is part of the Transportation Technology Center, Inc. (TTCI) in Pueblo, Colorado. The ERTC has provided in-depth hazmat emergency response training to more than 38,000 emergency responders and railroad and chemical industry professionals from all over the country and abroad. The ERTC is providing basic railroad safety and security training for 100 rail security inspectors hired by the TSA, and this summer ERTC will be training NJTTF personnel.

The ERTC is considered by many to be the "graduate school" of hazmat training because of its focus on comprehensive, hands-on training using actual rail equipment. TTCI boasts a collection of around 70 rail freight cars (including tank cars), some 15 rail passenger cars, 25 highway cargo tanks, van trailers, and intermodal containers, as well as computer work stations equipped with the latest emergency response software. TTCI is currently developing a Passenger Railcar Security and Integrity Training Facility to test the effectiveness of various response and remediation techniques in mitigating incidents involving passenger trains. This facility focuses on chemical, biological, radiological, nuclear, or explosive incidents and other activities associated with potential terrorist events.

Many members of Congress have had the opportunity to visit TTCI in person. I'm pleased to offer all members of this committee an open invitation to visit the facility to gain first-hand knowledge of its capabilities. On April 11, 2007, we plan to conduct a tank car test crash as part of an evaluation of tank car safety. This committee might want to consider scheduling a field visit to TTCI to view this demonstration.

The Rail and Public Transportation Security Act of 2007

As I noted earlier, railroads appreciate your interests in addressing rail security. As you consider specific legislation, though, we respectfully urge you to consider the extensive steps railroads have already taken to make our freight railroads more se-

cure. We also hope you remain mindful of the need to establish a proper balance between efforts to enhance security, on the one hand, and allowing the free flow of goods that is critical to our societal and economic health, on the other.

We also urge you to remember that any railroad security regime must take into consideration the nature of rail operations. Our freight railroads form a vast, overwhelmingly open system designed to move goods efficiently and cost-effectively throughout North America. By its nature, the system cannot be "closed." Moreover, in order to survive for more than 170 years, as they have, railroads have had to learn to be resourceful, flexible, and productive. Sudden disruptions brought about by weather, grade crossing accidents, rockslides, equipment failures, and countless other contingencies are a fact of life for railroads. I can think of no other industry that faces these kinds of disruptions as routinely, and typically handles them as well, as railroads do.

Consequently, this committee should keep in mind the impressive capabilities railroads have honed over the years in responding to unusual circumstances. We especially urge you to refrain from transferring key operational decision-making authority to a federal bureaucracy. Doing so would make it much more difficult for railroads to respond to and recover from challenges related to safety and security.[1]

Regarding specific rail-related provisions of the Rail and Public Transportation Security Act of 2007:

- *Section 3* calls for the Department of Homeland Security (DHS) to develop and implement a national strategy for rail and public transportation security. Railroads support this provision, particularly with respect to the mandate to develop a strategy to research and develop new technologies for securing rail transportation.
- *Section 5* requires DHS to issue regulations requiring railroads to conduct vulnerability assessments and prepare security plans. As discussed earlier, the rail industry is already well beyond the assessment stage. The legislation should make clear that DHS should review and may accept the security assessments and plans railroads already have in place to meet the requirements of this section.

  Section 5 also calls for the identification of a security coordinator "to require immediate communications from appropriate federal officials. AAR's members already maintain safety/security offices that are open around the clock, and the AAR maintains a 24/7 security emergency line.

  Section 5 also requires plans for locating shipments of railroad cars transporting "extremely hazardous materials or nuclear waste" that are "lost or stolen." With all due respect, the loss or theft of tank cars is not a problem in our industry. Railroads, at the request of the TSA, have agreed to provide movement data on all rail cars carrying toxic inhalation hazards (TIH).*
- *Section 6* requires DHS to develop a strategic information sharing plan to ensure the development of tactical and strategic intelligence pertaining to threats and vulnerabilities for dissemination to appropriate stakeholders. We support appropriate sharing of information. However, there should be clear and unequivocal protections to ensure that strategic information does not fall into the hands of those who would harm us.
- *Section 7* establishes a program for making grants to both passenger and freight railroads for infrastructure protection. We strongly support this provision, particularly the inclusion of "overtime reimbursement for additional security personnel during periods of heightened security" as an eligible security improvement. *
- *Section 11* requires DHS to develop a security training program for railroad workers and to issue guidance on such training to railroads. I address employee security training more fully below. It is important to note, though, that freight and passenger railroad environments are very different, and some elements of the employee security training program recommended in the bill (*e.g.,* element 5 on evacuation procedures) may be appropriate for passenger railroads but are not appropriate for freight railroads. Moreover, some elements of the bill (*e.g.,* element 1 on determining the seriousness of a threat) would require freight railroad employees to put themselves in harm's way, which contradicts existing freight railroad policies and procedures.

[1] The way railroads addressed the disruptions caused by Hurricane Katrina is illustrative of this point. Railroads prepared for the storm, assessed damage, and had most of their lines back in operation in the region in a matter of a few days. Again, rail industry preparation and response efforts were a model for everyone else.

• *Section 12* requires DHS to develop a program for conducting security exercises, including live exercises at railroad facilities. The railroad industry conducts regular table top exercises to ensure maximum continued effectiveness of its security plan. Railroads are concerned that live government exercises, if unannounced and not carefully coordinated with the railroads involved, could result in fatalities or injuries. To guard against this, we recommend that the provision be modified to require DHS to coordinate such exercises with railroads to ensure the proper safety of all participants in the exercises while on railroad property.*

• *Section 13* requires DHS to establish a research and development program for projects related to rail security. The AAR strongly supports this provision. On February 13, 2007, AAR offered testimony at a hearing of this Committee's Subcommittee on Appropriations. That testimony included a list of R&D projects that, if appropriately funded, would significantly enhance rail security. I attach this list as Appendix 1 at the end of this testimony.

Earlier in this testimony, I discussed the facilities available at the Transportation Technology Center, Inc., including the Emergency Response Training Center. Many of the projects outlined and recommended in the Rail and Public Transportation Security Act of 2007, and many other projects that are not mentioned but have important safety and security benefits, are already underway at TTCI. We urge you to utilize this unique and invaluable resource.

We also strongly support the provision that would make TTCI a member of the National Domestic Preparedness Consortium (NDPC), a group of premier institutions that develop, test, and deliver training to state and local emergency responders. Today, a facility specifically targeted at emergency response training for freight and passenger railroad environments is notably absent from the NDPC. Including TTCI in the NDPC offers a unique opportunity to improve our nation's ability to prevent, minimize, and respond to potential rail-related terrorist attacks.

• *Section 14* calls for new whistleblower protections, under the Department of Labor, designed to shield rail employees from retaliation for certain conduct involving issues related to homeland security.

Railroads do not object to equitable whistleblower protections for rail workers, but they do not believe that there should be one set of rules for whistleblowing on safety matters and a different set of rules for whistleblowing on security matters. The Federal Railroad Safety Act already has a whistleblower provision (49 U.S.C, Section 20109), and any expansion of rail employee whistleblower protections to include security should be undertaken within the context of Section 20109. Creating a new, separate system under the aegis of the Department of Labor is both unnecessary and potentially confusing, since situations could develop that could be handled under either Section 20109 or the Department of Labor.

With respect to Section 14, if the government invokes a states secrets privilege in a case where a railroad employee has filed a claim against a railroad, the railroad should not be precluded from presenting its justifications for any action taken against that employee, and the railroad should be able to obtain a judgment based on the justifications the railroad is able to provide.

• Section 15 would increase the number of non-aviation TSA inspectors from 100 to "at least 600" by the end of 2010. Railroads welcome the provisions specifying minimum qualifications for such inspectors and for requiring a clear delineation of responsibilities between TSA inspectors, FRA inspectors, state and local law enforcement, and railroad police. We are not convinced, however, that such an inspection workforce is necessary in the freight railroad environment, or that the new TSA inspectors would not simply duplicate the work currently performed by FRA inspectors. Railroads would prefer to see the limited resources available for rail security applied to the physical protection of personnel, critical assets, and the public.

• Section 16 establishes a National Transportation Security Center of Excellence (NTSCE) at an institution of higher education to conduct research and education and develop professional rail security training. We would hope that the work of the NTSCE and of other institutions associated with it would be integrated with the work underway at TTCI in Pueblo, Colorado so as not to duplicate efforts.

Railroads respectfully suggest that a number of other additional legislative provisions would enhance railroad security:

- Address the "bet the company" risk railroads must assume because of their common-carrier obligation to carry highly-hazardous materials, especially "toxic inhalation hazards" (TIH).
- Encourage rapid development and implementation of "inherently safer technologies" as substitutes for highly-hazardous materials, especially TIH.
- Ensure that any technology that is mandated to track and locate rail cars carrying hazmat and/or to identify actual or imminent hazmat release is fully proven, functional, reliable, and cost effective, and does not impede or endanger existing railroad systems.
- Make expenses mandated by the government (including mandates that result from high-risk corridor assessments) eligible for critical infrastructure protection grants.
- Allow police officers of one railroad to exercise law enforcement powers on the property of another railroad.[2]
- Engage the expertise and experience of rail industry personnel as significant domestic intelligence assets.

Many of the additional steps railroads recommend pertain to hazardous materials. Appendix 2 of this testimony contains an excerpt of AAR testimony offered on February 13, 2007, to this Committee's Subcommittee on Appropriations that discusses the hazmat issue in far more detail.

Rail Employee Security Training

Railroad 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, inspectors, and signalmen working along railroad rights-of-way; railroad police officers; and others. They are the "eyes and ears" in the industry's security efforts, and we should all be grateful for their vigilance and care.

The freight rail industry trains its employees to be vigilant, to report suspicious objects and activities, and to keep out of harm's way. The training has encompassed topics such as what to do when an employee sees a stranger or suspicious activity on rail property; to whom an anomaly should be reported; the need to keep information about train movements and cargos confidential; and the need to keep rail property secure and safe.

With 9/11, it became clear to railroads, as it did to firms in other industries, that security awareness would have to take on new importance. In response, Class I railroads soon thereafter provided a training video and/or printed materials to all employees—in most cases mailing the materials to employees' homes—that could be characterized as "Security Awareness 101." In the materials, the railroads expressed to their employees three fundamental expectations that to this day remain cornerstones of rail employees' responsibilities regarding security: don't put yourself in danger; report suspicious activities on or around railroad property; and don't divulge sensitive information about rail operations to others.

Over time, freight railroads began to incorporate security issues in a more formal fashion—for example, as part of employees' periodic FRA-mandated safety rules recertification, as part of new-hire training, and as part of new manager training. Many railroads have incorporated security issues into employees' manual of standard operating practices. Moreover, all railroads are compliant with U.S. DOT-mandated HM–232 security training for employees who handle hazardous materials.

More recently, railroads concluded that rail security would be enhanced if rail employee security training was more uniform across railroads through use of a standardized curriculum, and railroads have made that harmonization a reality.

Much has been done in collaboration with the National Transit Institute (NTI) at Rutgers University. NTI was established under the Intermodal Surface Transportation Efficiency Act of 1991 to develop, promote, and deliver training and education programs for the public transit industry. Freight railroads are fortunate to have been able to take advantage of NTI's success in promoting safety and security in public transit to develop an interactive, uniform security awareness curriculum for freight railroad employees.

The standardized curriculum has four modules: *What is Security; Vulnerability, Risk, and Threat; What to Look For; and Employees' Role in Reducing Risk.* The goal of the standardized curriculum is to provide rail employees with an understanding

[2] Such a measure was contained in legislation (H.R. 2351) introduced in the 109th Congress sponsored by Rep. James Oberstar, chairman of the House Transportation and Infrastructure Committee, and is included in S. 184 (the "Surface Transportation and Rail Security Act of 2007"), which is now included in S. 4 (the "Improving America's Security by Implementing Unfinished Recommendations of the 9/11 Commission Act of 2007").

of their role and responsibility in system security, and how to implement their companies' procedures upon detection of suspicious objects or activities.

For example, one module of the curriculum focuses on what system security entails in a general sense—*i.e.,* the use of operating and management policies and procedures to reduce security vulnerabilities to the lowest practical level, as well as a process focusing on preventing all levels of crime against people and property. Under a system security approach, rail employees are taught to realize that they and their duties are part of a larger, extensive system and that system security begins with the employee. To that end, employees are encouraged to be observant and to be familiar with their companies' policies and procedures in the event of a threat or incident.

Another module of the curriculum covers how to identify suspicious or dangerous activities. In the case of suspicious individuals, the focus is on behavior—specifically, where the person is, when he or she is there, and what he or she is doing. Railroads know that their employees know their daily work area better than anyone and are in the best position to determine if something looks wrong or is out of place. Thus, employee training emphasizes being familiar with the work area; observing and reporting suspicious activities and objects; reporting missing or malfunctioning equipment; and, if appropriate and endorsed by railroad policies, approaching and engaging persons to resolve or confirm suspicions. Rail employees are not to approach threatening people; try to intervene in dangerous activities; or pick up, touch, or move suspicious objects. They are expected to withdraw from dangerous environments and situations and are expected to report dangerous situations immediately.

As part of the standardized curriculum, employees are also trained how to react to threats, which may take the form of perceived suspicious activity, suspicious and/or out-of-place objects or vehicles, evidence of tampering with equipment, phone calls or other warnings, or other circumstances. Again, railroads do not expect their employees to "play the hero" by potentially putting themselves in harm?s way. Instead, they are expected to follow their company's policies and procedures, inform the appropriate authority of the situation, move to a safe location, and wait for further instructions.

We submitted our employee security training program both to DHS and to FRA for review and comment in February 2006. TSA reviewed the rail industry's training program, and advised us that it is "relevant and up-to-date" and is "helpful" in "rais[ing] the baseline of security-related knowledge." Recently, TSA inspectors surveyed 2,600 railroad employees and determined that 80 percent of the employees have a medium or high level of security awareness.

Class I railroads will complete security training for front-line workers (security personnel, dispatchers, train operators, other on-board employees, maintenance and maintenance support personnel, and bridge tenders) by the end of this year. Going forward, rail employee security training is being documented and records of it are being maintained.

As the information noted above makes clear, railroads treat very seriously their obligations in regard to security and have made sustained, earnest efforts to provide their employees with the tools and training they need to react appropriately when security-related issues arise. Moreover, railroads are not standing still in this regard. Through their efforts with NTI and others, railroads are continually refining their training efforts to improve their usefulness and effectiveness. Railroads are also always open to reasonable, constructive suggestions on how employee security training can be improved.

Criminal Background Checks

The legislation before you now includes a provision on criminal background checks that would apply to all covered transportation providers—railroads, public transportation providers, and over-the road bus operators. This provision is unwarranted, excessively broad in scope, and an intrusion into the rights of the industry to protect its workforce and property from convicted criminals. It is a reaction to a limited situation involving employees of railroad contractors that is already being appropriately addressed. Moreover, the legislation actually conflicts with the parameters prescribed by the regulatory regime set up for the U.S. government?s transportation worker identification credentials (TWIC).

On February 16, 2007, I testified before this Committee's Subcommittee on Transportation Security and Infrastructure Protection. In that testimony, I noted that railroads have an obligation to their employees, their customers, the communities they serve, and their shareholders to keep their personnel, their operations, and facilities as safe and secure as possible. Railroads take this obligation, which has taken on a new dimension in the post-9/11 world, very seriously. Like all other in-

dustries, railroads employ a variety of risk management tools to achieve this goal. One such tool is the use of criminal background checks of prospective employees and contractors seeking access to railroad property.

For any firm, the basic purpose of a criminal background check is to reduce the likelihood that a prospective employee will engage in workplace crime. Even when a conviction is not directly related to the potential duties of a position (*e.g.,* a conviction for embezzlement by an applicant for an auditing position), the conviction may be considered an indication that a necessary personal qualification (integrity, reliability, self control, etc.) is missing. Convictions of particular concern to railroads include crimes against persons, crimes involving weapons, crimes involving theft or fraud, and crimes involving drugs or alcohol.

There are also important liability considerations behind criminal background investigations. These include protection against lawsuits for "negligent hiring" and "negligent retention." Courts have ruled that employers can be held liable for the damaging actions of their employees, if, based on the employee's previous actions, he or she should have been disqualified for the position. Similar liability can arise from the actions of contractors and employees of contractors.

The above points all hold true for railroads. In addition, railroads face a growing body of requirements and recommended "best practices" related to homeland security that directly or indirectly call for criminal background checks for persons with access to rail property. These requirements and recommended practices emanate from DHS or one of its agencies, such as the TSA, the Coast Guard, or the U.S. Customs and Border Protection (CBP); from the DOT or one of its agencies, such as the Federal Motor Carrier Safety Administration or the Pipeline and Hazardous Materials Safety Administration; or from another government entity. Appendix 3 lists several examples.

A few years ago, the railroads determined that not all contractors working on railroad property were conducting background checks on their employees. To help close this gap, a nationally-recognized background investigation firm, eVerifile, was retained to create an industry-wide program known as e-RailSafe. The e-RailSafe program provides background checks and credentialing for the employees of contractors who need access to the property of Class I freight railroads.

The e-RailSafe program began in late 2005. To date, four of the seven Class I railroads are participating. Others have signed contracts with e-Verifile but have not yet initiated the program.

As I noted in my testimony on February 16th, when contacted by the Committee about some of the confusion surrounding the e-RailSafe program, we moved swiftly to clarify the rationale for the program and to provide a robust and responsive appeals process for contractor employees who were denied credentials due to their criminal backgrounds. A more complete description of the program and the appeals process is included in Appendix 4. Let me reiterate today that the background checks done by the railroad industry are conducted for a wide variety of basic, common sense reasons. As private property owners, we have a right—and an obligation)—to safeguard our personnel and property from persons with criminal backgrounds. If those background checks also help meet the recommended practices of the Department of Homeland Security, then all the better. But we strongly oppose the legislation before you that would severely constrain the ability of the railroads to protect its workforce and property.

Among our concerns with the provision are the following:

- It would apply not only to the employees of contractors, but to all employees of transportation providers.
- The provision is retroactive to background checks performed since June 23, 2006.
- The waiver and appeals process requires an ?independent decision-maker? with the ability to order reinstatement or provide other remedies. This is an intrusion into the rights of private companies to determine who it employs and who it allows on its property. As far as we are aware, no other U.S. industries are bound by a similar federal mandate.
- The disqualifiers specified are different than what is required by the DHS under its TWIC program. For example, while there are 11 permanent disqualifiers required by the TWIC, including murder, the legislation before you only includes treason, espionage and sedition.
- The timeframes for the disqualifiers in the legislation before you are also different from the TWIC. For example, this legislation would disqualify an applicant for credentials if he or she had a felony conviction within the last 6 years. A person applying for a TWIC card is disqualified if he or she has had a felony conviction within the last 7 years. This legislation would disqualify an applicant for credentials if he or she has been incarcerated within the last 4 years. A per-

son applying for a TWIC card is disqualified if he or she has been incarcerated within the last 5 years.

• As we have testified previously, our background checks do not use the same disqualifiers as does the U.S. government when it is considering an applicant for the issuance of security credentials. Our purposes are different.

• This legislation, for example, does not include the crimes of theft, drug use, or drunk driving as disqualifiers. In fact, the legislation would actually prevent a railroad from firing its own employees or denying property access to a contractor's employees found guilty of such offenses. The omission of drug use and drunk driving is particularly surprising given the stringent drug and alcohol testing program the federal government requires for railroad employees.

In short, this provision is a wholesale federal intrusion into the rights of private property owners to determine whom they can employ or have access to their property. We believe that the measures we are undertaking address this committee's concern that a process exist to give contractor employees a robust right of appeal.

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. Railroads 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.

Mr. THOMPSON. Thank you very much. Five seconds to spare.

Mr. Rodzwicz, thank you very much.

STATEMENT OF EDWARD W. RODZWICZ, PRESIDENT, TEAMSTERS RAIL CONFERENCE

Mr. RODZWICZ. Thank you, Mr. Chairman.

As president of the Teamsters Rail Conference, I appear today on behalf of more than 70,000 rail conference members who will be impacted by the proposed Rail and Public Transportation Security Act of 2007. Rail labor has taken every opportunity since 9/11 to advocate for strong security legislation for the railroad industry. And we are pleased to see that you have listened to what we have said.

The bill addresses many of the issues we have raised over the past five-and-a-half years. I want to comment upon a number of the provisions contained in the bill so that you have the benefit of rail laborers' view.

The Teamster Rail Conference is dedicated to improving rail security and safety in America in order to adequately protect rail workers and the communities they serve. Each and every day we are on the front lines of the nation's transportation system and see the woeful lack of security on our railroads. This lack of security is more than just troubling. It is tragic because we have seen the damage that can be done by accidents on the railroads and shudder to think of the damage that could be wrought by terrorism or sabotage.

Worker training is one area of grave concern for rail employees. The rail conference is most pleased with the strong requirements contained in section 11 governing security training programs for frontline railroad workers. The timeline appears appropriate to us. And we appreciate and look forward to consulting with the secretaries in developing these programs.

We wish to voice strong support for the requirement in subsection c8 that the program include training on understanding se-

curity incident procedures, including procedures for communicating with governmental and non-governmental emergency response providers. There is no question in our minds that this element will be strongly opposed by at least some management groups.

The conference also wants to voice our support for the whistleblower protections contained in section 14 of the bill. Railroad workers should not and cannot be subjected to dismissal when they provide security threat information to the government. These protections are absolutely necessary in order for our members to feel comfortable in the security environment this bill will create throughout the industry.

The proposed language strikes an appropriate balance between legitimate security needs for worker protection, the provisions for potentially stiff damages, and recourse to the judicial system to ensure that rail employees who blow the whistle on unsafe practices are afforded a fair forum for enforcement of their federal rights should their employer retaliate against them for protecting their fellow workers and the public.

Moreover, we are pleased with the subcommittee's adoption of Mr. Perlmutter's amendment which forcefully establishes that railroad workers who are subject to background checks are entitled to due process. These background checks already have cost at least a half dozen workers their jobs. And the Association of American Railroads was forced to concede last week that they did not have a process in place that would permit these workers to defend themselves.

As is the case with the whistle-blower protections, the rail conference believes there should be a single process applicable in all modes and that the Perlmutter amendment provides the process this committee should adopt.

Finally, while we view the bill positively in most respects, we wish to voice our concern regarding section 13, which addresses security research and development. Among the projects eligible for federally supported R&D are automatic inspection of railroad cars, and communication-based train controls which are included in subsections B(3)(b) and D(3)(c). Both of these subjects have been implicated in a most contentious round of collective bargaining that has not yet been completed for all of rail labor.

With respect to automatic inspection of railroad cars, we do not oppose research into technologies that could safeguard humans while assisting in conducting a security inspection of a railroad car. Indeed, we have voiced concern over unnecessarily exposing railroad workers to risk of injury or death while securely transferring certain hazardous material cars under proposed regulations. However, we adamantly oppose the use of federal funds to support research and development of technologies that would perform safety inspection of railroad cars.

As to communication-based train controls—and as you know, a major controversy arose last year when the industry attempted to gain the legal and political processes in order to eliminate a crew member on road freight trains via implementation of positive train control systems.

Federal support for R&D efforts to enhance security via communication-based train control systems in order to, for example, uti-

lize positive train control as a means of instantly locating a car carrying toxic by inhalation material, is an effort we would endorse. However, we oppose and caution the committee to not permit DMS to become ensnared in federally funded R&D efforts that facilitate the efforts of those who advocate crew size reduction.

Thank you, Mr. Chairman. And I am prepared to answer any questions.

[The statement of Mr. Rodzwicz follows:]

PREPARED STATEMENT OF EDWARD W. RODZWICZ

Thank you and good morning Chairman Thompson, Ranking Member King, and members of the Committee. My name is Edward Rodzwicz, and I am President of the Teamsters Rail Conference. I appear today on behalf of more than 70,000 Rail Conference members who belong to our constituent Brotherhood of Locomotive Engineers and Trainmen and Brotherhood of Maintenance of Way Employees Division, and who will be impacted by the proposed Rail and Public Transportation Security Act of 2007.

I want to begin by thanking the Chairman and the Ranking Member for the work they have done in putting together the bill. Rail Labor has taken every opportunity since 9/11 to advocate for strong security legislation for the railroad industry, and we are pleased to see that you have listened to what we have said. The bill addresses many of the issues we have raised over the past 5 1/2 years.

In my brief time today, I want to comment upon a number of provisions contained in the bill, so that you have the benefit of the view of the Rail Conference. For the sake of clarity, I will address those provisions in the order they are contained in the bill. Therefore, the order in which our points are made should not be interpreted as a prioritization of issues.

Section 5 covers rail and public transportation assessments and plans. Subsection (d)(1)(G) would require that Section 11 training include "recurrent training and periodic unannounced exercises for employees." The need for recurrent training for front-line railroad workers has long been a major theme for us, and we fully support conducting periodic unannounced exercises so that the sufficiency of security plans can be tested and in order for our members to better understand the goals and elements of their employers' security plans.

Subsection (g)(3) would require that the Secretary of Homeland Security, in consultation with the Secretary of Transportation, approve vulnerability assessments and security plans. We support a requirement that assessments and plans be reviewed and approved. It has been our experience that a mandatory approval process produces a much better product than a process whereby approval is deemed if the submission is not rejected within a certain time frame. It is our expectation that the industry will request an alternative to mandatory approval, and we strongly urge the Committee to retain the proposed language in the final bill. For the same reasons, we support the procedures, protocols and standards set forth in Subsection (k).

Concerning Subsection (l), which pertains to the periodic review of vulnerability assessments and security plans, we note that paragraph (1) mandates a periodic review within three years of the initial filing and at least once every five years thereafter. This schedule reflects the timeline proposed in parallel Notices of Proposed Rulemaking pertaining to rail transportation of certain hazardous materials, which were published by the Transportation Security Administration ("TSA") and the Pipeline and Hazardous Materials Safety Administration ("PHMSA") last December. In comments on these proposed rules, the BLET voiced a concern that the schedule for subsequent reviews was too long, and suggested that reviews be conducted triennially. *See* DOT DMS Docket No. TSA–2006–26514–59 at p. 4.

With respect to the rail security assistance grant program outlined in Section 7, we fully support the inclusion, in Subsection (b)(15) of security awareness, preparedness, and response training for front-line railroad employees, including Section 11 training, which also is reflected in Section 8(b)(14). Further, we applaud the Committee for the standards included in Subsection (h). Regarding eligibility standards set forth in Subsection (f), we are most grateful for the amendment offered by Congresswoman Clarke, providing that National Labor College, which is located at the George Meany Center in Silver Spring, Maryland, may be considered as a "private entity" in the application of paragraph (1).

Under labor sponsorship, the hazardous materials training programs at the National Labor College have been a resounding success. The program has, over its fif-

teen years, continually evolved and expanded to meet the training and competency needs of rail workers that are not met by the railroads. Initially offering only one course, the program now offers five. Training has moved beyond the conventional classroom to include simulation and on-line activities. A core of professionally trained instructors has been replaced with a corps of peer instructors. Because of this program's 16+ years of success, tens of thousands of rail workers are working more safely and in safer environments.

Since the onset of training in April 1991, the union-run program has trained more than 20,000 rail workers. Evolving from an 8-hour program of awareness training only, the National Institute for Environmental Health Sciences (NIEHS)-funded and George Meany Center-sponsored program now offers five courses: a 5-day Chemical/ Emergency Response training in the classroom; an on-line Emergency Responder Awareness Level 101 course; the OSHA 10-hour General Industry Safety and Health Outreach Program; disaster site training; and the newest addition, a Radioactive Material Transportation Safety Program, which is funded by a separate grant from the U.S. Department of Energy.

The newest program began last summer at the National Labor College, and includes a Modular Emergency Response Radiological Transportation Training (MERRTT) "train the trainer" course. By contrast, we are unaware of any railroad currently conducting training focusing on transportation of spent nuclear fuel and high-level radioactive waste, even though the Department of Energy is expected to begin a 38-year project to transport such waste from DOE sites to storage and disposal facilities as early as next year. The labor hazmat program has trained workers in 49 states and the District of Columbia. We also have fostered the creation of community partnerships that include joint rail worker, fire fighter, EMT, and public safety personnel training in communities throughout the U.S.

The progam has a new emphasis on railroad security and disaster response and teaches the five-day students about their role in serving as skilled support personnel in an incident command emergency setting. Much of the program material is available in Spanish and a comprehensive web site serves both the English and the Spanish-speaking work forces. The five-day program addresses the training requirements of the Department of Transportation's Hazardous Materials Regulations at 49 CFR Part 172, as well as the requirements of OSHA First Responder and Operations Level training under 29 CFR Part 1910.120. Railroads generally do not provide wages or support for workers attending the program. In fact,—and this is most unfortunate—members sometimes are not allowed time off from work to attend the program, even though the railroad is not paying wages.

The program currently serves eight rail unions,[1] and at least ten crafts,[2] from major railroads as well as from commuter and short-line railroads. This cross-company, cross-union, cross-craft training has proved invaluable, as one group learns from another. Each union has its own craft-specific tasks and challenges, and prior to this hazmat training program there was little, if any, cross-union training. Hazards and challenges faced by those in the yards may be different than those faced by road train crews, and different still from those who work along the track or in the shops.

Understanding the work of other crafts, the safety and health challenges that each face, and the coordination of each craft's efforts in an emergency, enhances railroad hazardous materials safety and security. A well-trained and knowledgeable workforce is the first line of defense and can prevent a minor incident from becoming a major hazardous materials accident. The eight rail unions have worked together to enhance rail safety by providing comprehensive training to its members and by providing substantial administrative and personnel support to the union-run Railway Workers Hazardous Materials Training Program.

Labor has been able to offer these programs through a combination of federal funds and subsidies from the North American Railway Foundation, which is a private non-profit organization. However, subsidies and contributions are hard to come by. Nonetheless, we take great pride in having trained over 20,000 railroad workers since the program's inception. At the end of the day, though, this represents but a

[1] Brotherhood of Locomotive Engineers and Trainmen (BLET); Brotherhood of Maintenance of Way Employes Division (BMWED); Brotherhood of Railroad Signalmen (BRS); International Brotherhood of Boilermakers, Iron Ship Builders, Blacksmiths, Forgers and Helpers (IBB); SEIU's National Conference of Firemen & Oilers (NCFO); Transport Workers Union (TWU); Transportation-Communication International Union (TCU); Brotherhood of Railway Carmen; and United Transportation Union (UTU).

[2] Brakemen, Laborers, Workers from the Building & Bridge Department, Signalmen, Carmen, Switchmen, Conductors, Track Department Workers, Locomotive Engineers, Yardmasters, and Hostlers.

small fraction of the front-line railroad workers who require thorough, in-depth training, and recurrent training.

We are pleased the Subcommittee concurred that the National Labor College qualifies as a "training partner," as that term is used in Section 648(a)(2) of the Department of Homeland Security Appropriations Act of 2007. See 120 Stat. 1427. Considering the NLC to be a "private entity" for purposes of Section 7(f)(1) of the bill will provide access to Section 7 grants, thereby facilitating Labor's ongoing efforts to provide world-class safety and security training to railroad workers.

We also wish to bring to the Committee's attention a difference in language between the rail and the public transportation assistance programs, and propose a resolution of that difference. Section (8)(d)(2)(A), addressing public transportation, requires that—in establishing security improvement priorities for recipients of assistance—the Homeland Security Secretary, in consultation with the Secretary of Transportation, also shall consult with the management and employee representatives of the designated recipients. However, Section (7)(c), which deals with the same subject for rail, provides only for a determination by the Homeland Security Secretary, in consultation with the Secretary of Transportation. We believe that rail security programs could benefit from the same broad stakeholder participation afforded in public transportation, and respectfully request that language similar to Section (8)(d)(2)(A) be incorporated into Section 7(c).

With respect to the fire and life safety improvements contained in Section 10, we are pleased that the issue of the tunnels on the Northeast Corridor finally will be addressed, after years of neglect because Amtrak has not been reauthorized since the late 1990s. Indeed, we appreciate that the Committee proposes authorizations over the next four years to deal with this issue. We point out, however, that the Senate's authorization bill for Amtrak—S. 294—currently provides significantly higher authorizations over this period. Therefore, we urge the Committee to support the greater amounts when this matter is taken up in conference.

We are most pleased with the strong requirements contained in Section 11, governing security training programs for front-line railroad workers. The timeline appears appropriate to us, and we appreciate and look forward to consulting with the Secretaries in developing the program. We wish to voice particularly strong support for the requirement in Subsection (c)(8) that the program include training on understanding security incident procedures, including procedures for communicating with governmental and nongovernmental emergency response providers.

There is no question in our minds that this element will be strongly opposed by at least some management groups. In this regard, we point to the recent decision by staff of the Securities and Exchange Commission to allow Norfolk Southern to exclude a Teamster shareholder proposal calling on the company to disclose its efforts to safeguard the security of its operations and minimize material financial risk arising from terrorist attack and/or other homeland security incidents.

We strongly believe the Commission's staff failed in its interpretation of "Ordinary Business" when it concurred with the Company's position that homeland security issues are strictly in the purview of management. It is absurd to equate issues such as the ramifications of a hijacking of a freight train carrying toxic or explosive materials with everyday management decisions such as setting shipping charges. It is our strong belief that the safety and security of our nation's rail network is a matter of national policy concern.

As you know, there have been more than 250 terrorist attacks on railroads worldwide in the past 12 years. The FBI has warned that our rail system is a likely target for terrorists and still the carriers are allowed to keep their security plans in the dark not only to their workers but also their investors and the communities in which they operate. The fact is that corporations can and do safely disclose information about actions taken to protect their infrastructure and personnel as well as associated costs. We have to look no further than Canada where the Canadian Pacific Railway discloses such information. We should settle for no less.

The Teamsters are appealing the staff's decision. We hope that the Congress and the Administration would encourage the Commissioners of the SEC to review and reverse the staff's decision. And we implore the Committee to hang tough when elements of Section 11 come under attack from railroads and other providers of covered transportation. Further, and for the reasons I stated before with respect to vulnerability assessments and security plans, we strongly support affirmative approval of security training programs, as required by Subsection (d)(2). We also believe that the one-year timeline for completing initial training contained in Subsection (d)(3) is adequate.

We wish to voice our concern regarding Section 13, which addresses security research and development. Among the projects eligible for federally supported R&D are "automatic inspection of railroad cars" and "communication-based train con-

trols," which are included as Subsections (b)(3)(B) and (b)(3)(C). Both of these subjects have been implicated in a most contentious round of collective bargaining that has not yet been completed for all of Rail Labor.

With respect to automatic inspection of railroad cars, we do not oppose research into technologies that could safeguard humans while assisting in conducting a **security** inspection of a railroad car. Indeed, we have voiced concern over unnecessarily exposing railroad workers to risk of injury of death while securely transferring certain hazardous materials cars under proposed regulations. However, we adamantly oppose the use of federal funds to support research and development of technologies that would perform **safety** inspections of railroad cars.

As to communication-based train controls—and as you know—a major controversy arose last year when the industry attempted to "game" the legal and political processes in order to eliminate a crewmember on road freight trains via implementation of positive train control systems. Federal support for R&D efforts to enhance security via communication-based train control systems, in order to, for example, utilize positive train control as a means of instantly locating a car carrying toxic-by-inhalation material is an effort we would endorse. However, we oppose, and caution the Committee not to permit DHS to become ensnared in, federally-funded R&D efforts that facilitate the efforts of those who advocate crew size reduction.

Lastly we want to voice our strongest support for the whistleblower protections contained in Section 14 of the bill. These protections are absolutely necessary in order for our members to feel comfortable in the security environment this bill will create throughout the industry. The proposed language strikes an appropriate balance between legitimate security needs and worker protection. The provisions for potentially stiff damages and recourse to the judicial system to ensure that rail employees who "blow the whistle" on unsafe practices are afforded a fair forum for enforcement of their federal rights should their employer retaliate against them for protecting their fellow workers and the public at large. Finally, we urge the Committee to stand fast on requiring a single process for all modes in providing these protections.

Moreover, we are pleased and thankful for the Subcommittee's adoption of Mr. Perlmutter's amendment, which forcefully establishes that railroad workers who are subject to background checks are entitled to due process. These background checks already have cost at least a half dozen workers their jobs, and the Association of American Railroads was forced to concede last week that they did not have a process in place that would permit these workers to defend themselves. As is the case with whistleblower protections, the Rail Conference believes there should be a single process applicable in all modes, and that the Perlmutter Amendment provides the process this Committee should adopt.

Once again, I thank the Committee for hearing us today on this important matter, and will be happy to attempt to answer any questions you may have.

Mr. THOMPSON. Thank you very much.

Mr. Weiderhold?

STATEMENT OF FRED WEIDERHOLD, INSPECTOR GENERAL, NATIONAL RAILROAD PASSENGER CORPORATION (AMTRAK)

Mr. WEIDERHOLD. Thank you, Mr. Chairman and members of the committee. I know we are on kind of a quick clock here so I will try to condense my remarks as much as possible.

First, I want to say thank you for probably what is the most significant piece of legislation for rail and transit since 9/11. It has been sorely missing in the overall approach that the country is taking with respect to mitigating security concerns in this nation. And I thank you personally and professionally for that, Mr. Chairman.

I have four quick points I would like to make for the committee. I don't have time to get into the detailed remarks on a section by section analysis. But they are included in my written remarks. And I would be most happy to respond to those at a later time.

The first point I would like to make is let me be one of those witnesses, at least, who is absolutely adamant about the point that I think the time that we need, the time that we are taking to respond to rail and transit security is running out. Most every wit-

ness you have that appears before this committee comes up and invokes Madrid and London and Mumbai, just as the members did in some of their opening remarks.

Those are wakeup calls. But I think in some quarters and some persons they reach over and hit the snooze alarm on the wakeup call button. Not everybody gets this yet.

Time is running out, Mr. Chairman. In your opening remarks, you pointed out that Madrid was almost 3 years ago. And in my personal opinion, we have come a little bit, we have moved the ball a little bit.

But we have not moved it far enough or fast enough. Your bill goes a long way in jump starting a lot of the initiatives that have been put on the back burner. And I appreciate that.

The second point I would like to make is that the committee really needs to capitalize and leverage the collective knowledge and experiences that cut across the departmental boundaries in the public and the private sectors. I know that the committees, both DHS and T&I are kind of wrestling with the language in the bill about consult versus coordinate. I would urge you to find the synergies that exist between and among both the members, the committees, and the departments that are out there.

There are very good people working this issue on both sides of the fence. And we need to find a way to absolutely capitalize on the talent that is out there.

The other point I would make is that there is really more good news out here than bad news. Commissioner Falkenrath brought up the fact that we have a working relationship with the NYPD. And Commissioner Kelly has been very forthcoming, very forward leaning. And we have a number of relationships like that between our company and local and state law enforcement that is really the model that the country should be using going forward.

I wish that the rest of the country was nearly as prepared as New York City is right now. New York City has a game face when it comes to protecting their transportation and transit assets. We do not have that across the country. It is sorely needed.

Another piece of good news is that we are kind of cross-pollinating personnel. Mr. Falkenrath comes from the NSC in the White House. He is now embedded in one of the major urban areas in the country leading the counterterrorism effort. Mr. Jamison, who I have worked with before, who I have a lot of respect for, has made the transition from the FTA to the TSA, which I think is a big plus.

Within Amtrak we have recently hired Jim McDonnell, who was the high ranking DHS official who was responsible for infrastructure protection. And we are hoping hiring people like that will help our handshake with DHS.

The third point I would like to make is you should ensure that the security standards and best practices are fully developed before we rush into regulations. 3 years ago, right on the heels of Madrid, TSA, DHS called us over, called over Amtrak, called over APTA, called over the freight industry. And we sat down and met with DHS to hammer out some security directives. Why did we have to do that. We had to do that because there were no security directives in place.

So over a period of time, a couple of months and a number of meetings with the principle operators and with the appropriate lawyers, we hammered out these security directives. They are good, but they are far from perfect. There are a lot of problems that exist with those security directives. But those were almost 3 years ago. And we have not iterated those directives yet to form the basis for the right kind of standards and the right kind of basis for regulations that would be forthcoming.

The other thing I would point to—and I think Mr. Millar intended to cover it in his testimony—is you need to look to organizations like APTA that are established security developments organizations, what we call SDO organizations. There is a lot of talent out here in the community. And we want both the Department of Homeland Security and the Department of Transportation to acknowledge and use that talent.

Finally, last point is—and it has been talked about among several of the witnesses. And that is this relationship between security and safety. I can tell you as a railroader for 30 years—and most of the people at this table who have been in and around the industry we get up every day. We have a safety message. We have safety training. We do safety inspections. It is a part of the fabric of our lives as railroaders.

Right now as we sit here, security is not on the same playing field as safety. I would encourage you at every turn not to bifurcate, not to delink safety and security. So where you have the opportunity to, again get some synergy between the two of those functions, please do.

I am prepared to answer any questions that you may have on the written testimony. Thank you.

[The statement of Mr. Weiderhold follows:]

PREPARED STATEMENT OF FRED E. WEIDERHOLD

Thank you for the opportunity to appear before you today to discuss rail security issues and the Rail and Public Transportation Security Act of 2007 draft bill. I share the Committee's concern and sense of urgency that much more can be done to secure and safeguard our nation's rail and transit assets. The responsibility to act is shared among federal, state, and local governments, and the private sector, and your bill will help jump start some long overdue initiatives.

You have heard testimony from many witnesses about the complexity of the rail environment, the challenges to secure such an 'open system', and the need to balance vulnerabilities, threats, and risks in allocating federal security dollars—these are real challenges. Having worked intimately with passenger rail safety and security issues for over twenty years, I will tell you the work to secure the railroad is very difficult, and often frustrating; however, I will also tell you that collectively we can greatly improve our readiness.

Before offering specific comments on the draft bill, I would offer some over-arching observations for your consideration:

• **The time to take action to possibly prevent, mitigate, and recover from a terrorist attack involving rail and transit assets is quickly passing—we need to act now.**

The reality, as the Committee Members are very well aware, is that we are operating our rail services in the wake of Madrid, London, Mumbai, and other cities where terrorist have elected to wage their war. I suspect that every witness who testifies before you about rail and transit security will invoke the names of the cities attacked, but how much have we really accomplished over the past several years—clearly, not enough. The Committee has received testimony from the GAO regarding delays to the Transportation Sector Specific Plan, and the Committee is taking action to ensure better coordination of transportation security strategies and plans. Amtrak is not waiting; its Board, its new Chief Risk Officer, and management have

made new commitments to increase significantly its canine resources, place more of its own, and other, police and security on its trains and in its stations, review its screening protocols, re-direct capital monies to critical asset protection, and 'build-in' security wherever possible. Your bill, and the specific inclusion of funds to address Amtrak?s security investment needs, is welcome and appreciated.

• **Capitalize and leverage the collective knowledge and experience that cuts across Departmental boundaries and the public and private sectors.**

Your bill requires greater cooperation and real coordination between and among those Departments and agencies with responsibilities for homeland security; this is a great message. It is an understatement to say we are not using all of our resources optimally. The GAO has commented that the sheer number of public and private stakeholders, and the complexity of our rail systems, may lead to duplication of effort, communications challenges, and confusion about roles and responsibilities—that has happened. The good news is there has been some progress—in well executed, risk-based vulnerability assessments, in meaningful state and local law enforcement cooperation, in emergency response training, in advancing security technologies (helpful, but not a panacea), and, mostly, in very good people stepping forward, trying very hard to work the issues. DHS and DOT must continue to reach out and tap these resources, and rail and transit security should not be compromised or relegated to turf struggles.

• **Ensure security standards and best practices are fully developed before regulations are promulgated.**

One of the difficulties we have encountered in evaluating Amtrak's efforts to improve its security posture is the lack of security standards that have been fully vetted, practiced, and iterated. Although some security directives were prepared by TSA in May 2004, these directives are not necessarily the comprehensive bases for an effective rail passenger security strategy or effective regulations. The Committee may want to direct a joint Department review of the effectiveness, lessons learned, and potential enforceability, of the existing TSA Security Directives (RAILPAX 04–02) before additional directives are enacted.

The Committee should look to organizations like APTA, which is recognized as a Standards Development Organization, as a starting point to develop baselines for rail security and emergency preparedness best practices. Amtrak also is re-examining its protocols and will most likely redefine its own baseline security standards, working closely with domestic and international rail and transit partners, as well as DHS and DOT.

• **Ensure linkage between security and safety.**

One of the definitions we are using within Amtrak to determine when we have achieved adequate security awareness is when security has the same status as safety on our railroad. All rail operators—be they freight, passenger, or transit—live and practice safety in their daily work lives. Railroaders begin their day with safety messages and safety inspections; we train for it, we measure it, we have recognition ceremonies to celebrate it, and we do not take it for granted. In the new world of terrorism, especially terrorism directed at rail and transit, the same must become true for security. Certainly, there are protocols, practices, and skill sets that differentiate security from safety, but the work is performed over the same assets and the same operations. Whenever possible, security and safety should be addressed concurrently.

Specific Comments for Draft Bill:

Section 3—National Strategy for Rail and Public Transportation Security

This section requires that the Secretary of the Department of Homeland Security (DHS), in consultation with the Secretary of the Department of Transportation (DOT), develop a comprehensive modal plan for covered transportation. While consultation is certainly a prerequisite for effective working relationships between the two Departments, there will also be occasions where close coordination is required, where interdepartmental, cross-functional teams should be established, and where joint operations may be warranted.

At Section 3 (a) (4), the Committee includes a requirement that DHS and DOT develop a process for expediting security clearances and facilitate intelligence and information sharing. The Committee may wish to prioritize this requirement by mandating an expedited security clearance process for select senior rail and transit officials (CEO, COO, Chief Security Officer or equivalent) for all carriers assigned to the high risk tier. Senior railroad officials have had to wait well over one year for such clearances. Additionally, the Committee may want to direct that the processes for facilitating intelligence and information sharing be evaluated by the Department OIGs.

VerDate Nov 24 2008 14:16 May 21, 2009 Jkt 000000 PO 00000 Frm 00086 Fmt 6633 Sfmt 6621 H:\DOCS\110-HRGS\110-12\35271.TXT HSEC PsN: DIANE

At Section 3 (a) (7), the Committee requires that the joint modal plan include, "a framework for resuming the operation of covered transportation in the event of an act of terrorism and prioritizing resumption of such operations". This directive is highly significant because it requires DHS and DOT to become attentive to continuity of operation planning, not just for individual carriers, but for transportation systems.

Section 4—Assignment to Risk-Based Tiers

We agree that it is extremely important to establish criteria by which those carriers and systems that face the greater risks are prioritized. Terrorists' strikes against rail targets have historically involved light rail passenger systems and transit, often focusing on multiple targets, and, as we saw in the London bombings, follow-up attacks on connecting bus services. For these reasons, we encourage assignment based on modal and inter-modal "systems" as well as individual providers within those systems.

Section 5—Rail and Public Transit Assessments and Plans

We agree with the Committee?s direction to mandate vulnerability assessments and security plans for the rail sector. We know the Committee will find many carriers have already completed such assessments, and security plans have been prepared and are exercised during heightened threat levels.

Using DHS Office of Domestic Preparedness (now Grants & Training) funds, vulnerability assessments for Amtrak's Northeast Corridor and Chicago Union Station were completed in May 2006. Vulnerability assessments for the balance of most of Amtrak's other system assets should be completed this fiscal year. The methodology used for Amtrak's vulnerability assessments are consistent with that used for the majority of the transit properties. We believe these assessments, while not exhaustive, provide a valuable mapping of the vulnerabilities of key Amtrak, and Amtrak-used, assets, but these are only starting points.

The Amtrak OIG has observed that many of the vulnerability assessments are carrier-specific and not necessarily linked to larger system or nodal vulnerabilities. An appropriate role for a DHS Area Rail and Public Security Committee, or larger DHS entity, would be to link the assessments and plans into a larger rail transportation security matrix.

An interesting provision that the Committee recommends in Section 5 (f) is for Security Performance Requirements (for the security plans). We presume the performance requirements are intended to answer the question of 'how effective' the security plans are in adding to value to security preparedness. These performance requirements may evolve into the 'successor' guidelines to the RAILPAX Security Directives.

The Committee, and DHS and DOT, need to appreciate the complexity of the passenger rail operating environment and impact on stakeholders with respect to conducting vulnerability and threat assessments and preparation of security plans. For example, Amtrak serves over 500 rail stations across the country, but owns less than 80. Initially, Amtrak began its vulnerability assessments of Amtrak-owned properties, and, only later, expanded its assessment approach to include other 'Amtrak-used' assets. Even using an "owned assets" approach, there are difficulties in implementation with the myriad of stakeholders sometimes present.

For example, here at Washington Union Station, part of the facility is directly owned by Amtrak (from the gate areas north), the Main Hall and retail facilities are owned by the Union Station Redevelopment Corporation (USDOT, Amtrak, DC), areas of Columbus Circle are owned/controlled by the U.S. Park Police, Capitol Police, and the District of Columbia. In addition, Virginia and Maryland operate state-supported commuter services into the station (using both Amtrak and CSX operating crews and equipment). Which entity should have responsibility for vulnerability assessments and security planning for a complex property or inter-modal facility?

Given the criticality and iconic value of an asset such as Washington Union Station, Amtrak, appropriately, elected to undertake assessments that involved all property owners, all operators and users, and other stakeholders. At other stations and facilities, it may be less clear.

Section 6—Strategic Information Sharing

The goal of this requirement is to develop an information sharing plan to ensure the development of both tactical and strategic intelligence products for the rail sector, with special attention being paid to the coordination of intelligence analyses between TSA and other intelligence groups. We agree with this recommendation.

Amtrak has access to several sources of intelligence information today, both through DHS and DOT, as well as through other sources. Amtrak participates in

the Surface Transportation Information Sharing and Analysis Center (ST–ISAC), which was established and is maintained by the Association of American Railroads (AAR). The ST–ISAC provides useful information to Amtrak, especially in the areas of cyber-security and after-action threat analyses. Amtrak also participates in the Railway Alert Network (RAN), another AAR-maintained information and intelligence sharing system.

More recently, Amtrak placed personnel on the FBI's New York and Washington Field Office's Joint Terrorism Task Forces (JTTFs), and the National Joint Terrorism Task Force (NJTTF), with access to those units' intelligence centers. Additional Amtrak and OIG staff are assigned to various Department of Justice sponsored Anti-Terrorism Advisory Councils (ATACs) and working groups.

I would rate the dissemination of unclassified information, For Official Use Only (FOUO), and Sensitive Security Information (SSI) to Amtrak as good and improving. However, we absolutely share the AAR?s concern about the critical need to safeguard and compartmentalize all classified information, including SSI.

With respect to Section 6 (e), regarding the relationship of Security Clearances to intelligence information dissemination, the Committee and DHS may want to consider greater use of intelligence 'tear sheets' to disseminate more critical information. Additionally, the Committee and DHS should be concerned about the availability and use of classified communications channels with rail sector officials.

The Committee should also be cognizant of the fact that rail service providers, when conducting vulnerability, threat, and risk analyses, as well developing security plans and mitigation and response strategies, are generating a considerable amount of highly sensitive data that can be easily exploited to the provider's, and the nation's, detriment. Amtrak has taken advantage of DHS's Protected Critical Infrastructure Information Program by submitting work product for protection under the Critical Infrastructure Information Act.

Section 7—Rail Security Assistance

Amtrak strongly supports its inclusion as an eligible entity for security improvement grants. A stable funding mechanism for sustained security and emergency preparedness improvements at Amtrak, and within the passenger rail sector, is critically important.

Most of you know that Amtrak's financial condition has been precarious in recent years, and Amtrak's funding of police and security operations has been limited to its own internal police forces (about 350 persons) and work on a major fire and life-safety tunnel project in New York City. Amtrak was requested, on several occasions, by both House and Senate Members to delineate what it needs to advance its security and emergency preparedness, but well intended bills have never been enacted.

Since FY 2005, Amtrak has been allocated only about $22 million in DHS grant funds. Amtrak has used some of these grant funds to conduct vulnerability assessments, install a pilot chemical sensor system in four stations, fund a Washington, DC tunnel security pilot project, and fund several other higher priority projects. However, there are many more security and emergency preparedness projects and initiatives for Amtrak that require the support contemplated by the Committee?s bill.

In addition to those grant funds available to Amtrak under the Committee's bill, Amtrak's Board of Directors and its senior management are committed to doing as much as possible within the limits of Amtrak's internal finances. Amtrak's new Chief Risk Officer, a former high ranking DHS manager, has requested that Amtrak increase its canine units and work immediately to get more police and counter-terrorism security forces riding its trains. Amtrak has had great difficulty in filling its police and security staffing levels because its pay and retirement benefits are well below those of competing jurisdictions, resulting in double-digit attrition and a high vacancy rate. The Chief Risk Officer is working closely with Amtrak?s authorizing committees to find relief for this most serious problem.

Section 10—Fire and Life Safety Improvements

We strongly support the Committee's recommendation to provide additional grant authority to address security issues involving Amtrak's Northeast Corridor tunnels.

The New York City, Baltimore, and Washington DC, underground and underwater tunnels present special safety and security issues for Amtrak.

In New York City, over 1,100 trains daily use the 81,000 feet of tunnels into out of the City, with Amtrak and New Jersey Transit using the North River Tunnels beneath the Hudson River, and Amtrak and Long Island Rail Road using the East River Tunnels.

The scope of Amtrak's current Life Safety Program, valued at $470 million for Phase One, with a completion date of 2009, encompasses the construction of three major ventilation structures in Weehawken, New Jersey, Queens, New York, and

Manhattan. Also included in this project is the installation of a fire standpipe system throughout the New York Penn Station complex. The Weehawken Ventilation plant was placed into service in January 2005, and the dry standpipe was placed into service in January 2006. Through December 2006, $279.6 million has been spent on this project, funded through Federal Railroad Administration grants, the Long Island Rail Road, and Amtrak.

Amtrak's Northeast Corridor rail services and Maryland Transit Administration's MARC services pass into the heart of Baltimore through a series of tunnels, which were constructed in 1872. The Baltimore & Potomac tunnels house vital electric power lines and are critical to Amtrak's mainline operations.

With regard to the First Street Tunnel here in Washington, DC, Amtrak is working closely with DHS and is participating in the National Capital Region's Rail Corridor Pilot Project program. This project, which has proceeded much more slowly that I would have hoped, is one which I would like to brief to the Committee at a later time.

Section 11—Security Training Program

There is no substitute for having a well trained work force who can serve as the 'eyes and ears' and who act as the first line of defense in noticing suspicious activities and things that are 'out of place' on our railroad. Likewise, we need an alert and vigilant public, who know what to do and how to act before and during emergencies, and how to report to matters that warrant the carrier's attention.

Amtrak has followed the Federal Transit Administration's and the American Public Transit Association's lead in developing employee awareness training. Using security awareness training developed by Rutgers University National Transit Institute (NTI) for mass transit employees in 2003, the NTI's transit training modules were modified slightly and customized to address Amtrak's facilities and rail environment. An introductory and mandatory block of four hours of security training, including some class, Web-based, and CD-based training, was delivered to all Amtrak employees (17,000+) in FY 2006. This training was intended to be equivalent to "Security 101" for railroad workers. An additional four-hour, instructor-led block training for up to 14,000 employees is being delivered in FY 2007, with the first classes started in January 2007. My Office reviewed this training, and we believe that it provides a good foundation of security awareness from which additional, more specialized training can be targeted for select employees. One of the challenges for security training is to keep it topical, customize the training for the scope and responsibilities of the employee's position, and reinforcing the training through meaningful exercises.

Amtrak has also begun a limited version of the popular "see something, say something" program that is used by a number of transit properties. Amtrak has implemented a station and on-board announcements program, alerting the public to have control of their personal baggage and carry-on articles, and to report suspicious behavior during high threat levels declared at the national level. This program is being expanded to be a part of Amtrak's normal business practice.

With regard to Section 11 (c) (3), requiring inclusion of "appropriate responses to defend oneself, including using non-lethal force," as a part of employee security training, we believe this requirement may run counter to prevailing best practice. Amtrak, and most other carriers, recommend that employees, unless trained as police or full-time security staff, avoid physical confrontation, but instead be aware of their surroundings and contact qualified carrier and/or law enforcement personnel at the earliest opportunity.

Section 12—Security Exercises

Most carriers, including Amtrak, have considerable experience with emergency response drills and exercises, with greater frequency of such activities since 9/11. There is a growing body of 'lessons learned' from the exercises, drills, and table-tops, and resulting after-action reports that assist in safety and security investment decisions, and facilitate changes in operational protocols.

From an OIG perspective, I have seen very well conducted and useful security exercises, and I have also seen poorly executed, artificially constrained, and little value added exercises. More importantly, I have seen very meaningful recommendations from exercises and assessments that have not been timely acted upon. I very much support the inclusion of the Remedial Action Management Program, using FEMA's experiences, in monitoring implementation of lessons learned and best practices. My Office will also be monitoring the adoption and application of observations and recommendations generated by security exercises.

Section 13—Security Research and Development

The Committee has recognized the need for more collaborative research and development and technology convergence to develop affordable and effective rail security solutions; we very much agree. There are considerable challenges for passenger carriers to find and apply the most appropriate security technologies to fit their environments. Much of what has been accomplished to date by passenger rail is accomplished by information exchanges through existing industry associations and through professional relationships and private sector marketing. There has been some assistance provided by DHS in the form of providing screening equipment for pilot projects and special security events, but much more can be done in this area.

It is appropriate to recognize important work being done in security technology advancement by the rail industry. The AAR maintains a Transportation Technology Center (TTCI) in Pueblo, Colorado, which is used for both testing and training purposes; Amtrak routinely uses TTCI services. We support the Committee?s adoption of the amendment to make TTCI a member of the National Domestic Preparedness Consortium (NDPC).

Amtrak has also established relationships with the Lawrence Livermore National Laboratory, working with the OIG to conduct CBRNE assessments at ten major urban stations; with Argonne Laboratories, to install chemical sensor technology; and with Minnesota State University to install a SMART CCTV system at four stations. Amtrak, and the Amtrak OIG, have also benefited from the work and ongoing support of the Technical Support Working Group in making critical vulnerability assessments of key passenger rail assets.

Section 14—Whistleblower Protection

We very much understand the desire of the Committee to protect and safeguard those who would come forward to report violations of security-related statutes and regulations. Whistleblower statutes are intended to encourage vigilance using our greatest resource, our employees, by protecting them from retaliation and discrimination for such reporting.

As an Office of Inspector General, my Office responds to whistleblower allegations under the Railroad Safety Act; we also investigate allegations of harassment and intimidation under 49 CFR 225, regarding Railroad Accident Reporting. Additionally, under the Inspector General Act, we have responsibilities that are analogous to whistleblower protection applicable to Amtrak employees.

From our reading of the draft bill, and from an Amtrak OIG perspective, there does not appear to be any precedential equivalent to the allowable damages and criminal penalties for violations of this provision. The Committee may want to extend further inquiry into this area as well as be briefed on the extant DOT whistleblower statutes and regulations, including 49 CFR 42121, which involves whistleblower protection of employees providing air safety information, and applicable DOT reports on whistleblower cases.

Other Recommendations:

- Authorize railroad police officers to exercise law enforcement powers on the property of another railroad. This would allow railroads to better leverage their police and security assets. The proposal was included in earlier legislation from the 109th Congress, sponsored by the House Transportation & Infrastructure Committee.
- With regard to the Committee's proposed directives on background checks, we agree that September 11 altered the vigilance which we all must employ in the transportation industry with respect to third parties as well as employees and contractors. Thus the issue of background checks of certain employees is a somewhat complex issue, yet a critical piece of the cloak of security. The difficulty lies in the determination of **which** employees should be subject to background checks and **what should be considered disqualifying factors.** In managing a personnel security program, the following factors are vital: assigning risk designations for all employee positions; determining who completes the background checks (carrier/DHS/DOT); determining which background check system is most appropriate (when should NCIC be allowed); ensuring that the background checks are timely and thorough; establishing controls to protect against terminations that are based upon inaccurate or stale information, including the right to submit promptly rebutting information (Amtrak fully complies with the Fair Credit Reporting Act, which already provides a level of protection for individuals to challenge inaccurate information contained in a background check); adopting document control policies for personnel security files; and, ensuring that those performing background checks are properly trained and audited.

For instance, some of the criteria for assessing risk would be unescorted access to secure areas, potential for dangerous activities or compromising one's duties and

responsibilities, potential for greatest harm to passengers or human life, and the degree to which oversight can be exercised with respect to such personnel. Amtrak engineers who operate the trains, mechanical personnel who inspect, analyze and repair safety critical parts such as brakes, personnel who work in rail traffic control facilities, and baggage handlers would perhaps all be designated as requiring higher security clearances and the more extensive background checks. Under any contemplated program, carriers would be required to submit its comprehensive plan to be approved by either the Department of Homeland Security or the Department of Transportation.

Background: Amtrak Office of Inspector General

The Amtrak OIG is a fully statutory designated federal entity OIG established by the Inspector General Act of 1978. The OIG was established in 1989, has about 100 employees, and operates from seven field offices throughout the United States.

The OIG is responsible for oversight of all of Amtrak's programs and operations. For the past several years, the OIG has been heavily involved in evaluating and overseeing security operations within Amtrak. Immediately following the bombings in Chechnya, in December 2003, Amtrak's Board Chairman asked me to conduct an in-depth review of Amtrak's police and security operations. My Office worked with the Federal Railroad Administration (FRA) to obtain the services of the RAND Corporation to conduct this review. We were barely one month into our work when terrorists struck the Spanish rail system on March 11, 2004. In May 2004, we provided Amtrak with our observations and recommendations to improve security preparedness and to formalize and upgrade its police and security planning and operations. Amtrak has made some progress toward addressing some of the security shortfalls that were identified, but significant challenges remain.

We have been very forward leaning in our security assessments. During the past two years, my Office has conducted several 'red team' operations covering critical Amtrak assets; we have performed detailed CBRNE site assessments using the Lawrence Livermore National Laboratory Homeland Defense Operational Planning System (HOPS) group; we have been greatly assisted by the California National Guard and the Technical Support Working Group (TSWG) in contracting for highly detailed, virtual digital mapping of key stations (for use by asset stakeholders and first responders); and we have been similarly assisted by the National Guard Bureau and their Full Spectrum Infrastructure Vulnerability Assessment (FSIVA) teams. We have also independently contracted and sponsored counter-surveillance training for select Amtrak police, OIG staff, and other railroad security staff. In short, we on our own have sought help from almost any quarter, be it federal, state, and private entities, to find those "right things" to do.

My Office and Amtrak also reached out to the international rail and security communities, sponsoring visits in February 2005 from the Guardia Civil, Spain's premier counter-terrorism unit and Spain's national railways operator, Renfe. In 2006, Amtrak officials were briefed by both British and Indian Railway officials regarding attacks in their countries, and as recently as last month, Amtrak senior managers were provided special briefings by the British Transport Police.

Another important development affecting Amtrak's Northeast Corridor was the creation of Northeast Rail Police Coalition. Last year, NYPD Commissioner Ray Kelly called for a summit of police chiefs and other high ranking law enforcement officials from New York City to Washington DC. Commissioner Kelly proposed a coordinated approach by city, state, and local law enforcement to improve passenger rail security. The group, comprised of NYPD, Amtrak Police, Baltimore City Police, Delaware State Police and Delaware Homeland Security, Metropolitan DC and Transit Police, New Jersey Transit Police, Philadelphia Police, and other New Jersey and Pennsylvania State law enforcement, agreed to provide periodic support to Amtrak by boarding trains with officers and bomb dogs at key stations, conducting surveillance of the track and other facilities, and conducting other protective measures. This coalition began their work starting in July 2006, and we are pleased to report has become an integral part of Amtrak's security operations.

The Amtrak OIG has also joined the President?s Council for Integrity and Efficiency (PCIE) Homeland Security Roundtable, chaired by DHS Inspector General Richard Skinner, where we will be sharing red teaming and other security assessment approaches with the OIG community. And we will begin using the PCIE's *Guide to Evaluating Agency Emergency Preparedness (November 2006)* in our FY 2007 and FY 2008 evaluations of emergency planning at Amtrak.

We have had extensive involvement in the rail security and the anti-terrorism field.

Mr. THOMPSON. Thank you very much.

Welcome, Mr. Shuman. Please.

STATMENT OF DAVID SHUMAN, PRIVATE CITIZEN

Mr. SHUMAN. Thank you, Mr. Chairman. I am pleased to have the opportunity to appear before you today to talk about a threat that should be specifically addressed in the proposed security bill. And that threat pertains to the continuing vulnerability of cities to the intentional release of rail transported ultra-hazardous materials.

Now, enactment of the bill would clearly lead to a significant improvements in several areas, especially as that it would ensure that dollars and not just lip service stand behind our commitment to oppose threats behind box cutters and shoe bombs. But it also bodes well that the bill's 18 identified uses of rail security assistance funds are spot on in order of priority. But the bill needs to do more.

Five weeks ago on January 28th, a dump truck with explosives and a chlorine tank blew up in Ramadi killing 16. On February 20 and 21, two similar attacks killed 11 and wounded 180 near Baghdad after an al-Qa'ida chlorine bomb factor was discovered, military spokesmen expressed shock over the brutality of the weapons and the fear that with experimentation and more learning the bombs would become far more deadly.

Now, at a moment when al-Qa'ida is turning its attention to the potential of chlorine, it is worth renewing a serious look at this threat. Terrorists know they will only get one crack at tank cars. They will intend to make full use of that one opportunity. And we can deny them that opportunity only by severely restricting the movement of ultra-hazardous materials through those places where an attack will be worth the terrorists' while. And that is in high-density urban corridors.

Railroads will not do this of their own accord. And this has been aptly demonstrated by the industry's reaction to the D.C. HAZMAT ban. The burdens on interstate commerce and massive disruptions of rail operations that the industry posits is far from likely to occur only one in 3,200 of CSX's cars were even affected by that ban.

Meanwhile, the Pipeline and Hazardous Materials Administration has proposed rules this past December that, in fact, do leave all questions as to routing up to the railroad's own discretion. It is expressed in the rules ultimate decision making power is left to their judgment and their judgment alone. The carriers are also advised by the administration not to consider alternative routes that could involve the tracks of another railroad.

The agency's proposed rules have been represented by DOT Secretary Peters to accomplish one thing: establish a scientific system for determining where and when alternative routing of HAZMAT should occur. While, in fact, it is intended to do something quite different: provide political cover for any railroad resisting pressure to reroute.

The plan would create a federally mandated black box procedure with data selection, analysis, and interpretation of results all performed by the very parties, affected railroads, that are meant to be governed by the outcome. The 27 factors proposed to evaluate alternative railroads are custom designed to revalidate pre-existing operations.

Carriers are told to make their decisions based on "the financial management principles generally applied to other business decisions." The full text is no less startling than an EPA rule which would require electric utilities to install pollution controls but only if compliance produced greater profits without raising rates.

Several little factors serve to tilt results towards existing routes with no anti-terror justification whatsoever. And to provide a pattern of legitimacy, one factor to be considered is population density that is probably balanced out by another superficially innocuous factor, the extent of emergency response capabilities along the route.

Now, where would these greatest capabilities be? Where there are most people, one presumes. AAR standards require higher inspection frequencies on major HAZMAT routes. Thus the methodology asks how frequently are the tracks inspected. You can guess where the high frequency of inspections is more likely to occur on routes where HAZMAT now moves or on alternative routes where it does not.

There will be no opportunity to challenge railroad decisions as the entire decision making process would be considered SSI. It is hard to believe that this is all meant to pass as a serious methodology applicable to any legitimate public purpose. I recommend in my prepared statement a number of conditions under which tank cars with TIH would be allowed to enter city course.

Thank you.

[The statement of Mr. Shuman follows:]

PREPARED STATEMENT OF DAVID SHUMAN

Good morning Chairman Thompson, Ranking Member King, and Members of the Committee. I am pleased to have the opportunity to appear before you today to talk about an issue that is of great concern to many of us who live or work in the Nation's Capital or in any of a host of other major cities throughout the country. That issue is the continuing and worsening vulnerability of our cities to the intentional release or detonation of rail-transported ultra-hazardous materials.[1]

The proposed Rail and Public Transportation Security Act of 2007 (Rail Security Act or Bill) would provide a vehicle which will mandate the preparation of vulnerability assessments and security plans by surface transportation providers, require that these plans actually meet meaningful standards, and backs these mandates with strong incentives to encourage compliance.[2] All well and good. The Bill proposes to get major actors organized, become aware of their responsibilities, and critical lines of communication. This is also good. It is past time that some order supplant a *laissez faire* system characterized by endlessly circulating drafts of interagency memorandums of understanding. And of greatest consequence, in my view, enactment would ensure that dollars, not just lip service, stand behind the our response to transport-related security threats other than box cutters and lip balm. It also bodes well that in terms of cost-effectiveness, the Bill's eighteen identified uses of rail security assistance funds are spot-on in order of priority.

But there is one thing that the Bill could do, should do, but which it does not do. And that is to preserve all useful and viable options that may be employed to reduce the threat that weaponizable railroad tank cars, especially those laden with toxic inhalation hazards (TIH) such as chlorine, pose to major population centers.

[1] 1In addition to the District of Columbia, legislation to ban ultra-hazardous shipments has been introduced in Chicago, Boston, Philadelphia, Cleveland, Baltimore, St. Louis, Albany and Buffalo.

[2] The Pipeline and Hazardous Materials Safety Administration's (PHMSA) Notice of Proposed Rulemaking (NPRM) indicates that standards-based planning as contemplated in the Bill is not viewed favorably by all potential affected service providers: "Commenters are nearly unanimous in opposition to requirement for DOT and DHS to review and approve specific security plans, unless done on-site as part of a compliance or outreach review." 71 FR 76838, December 21, 2006.

The option in danger of succumbing to misguided administrative action and which the Rail Security Act should expressly revitalize is the authority, exercisable by a public entity, to prohibit railroads from moving loaded ultra-hazardous tank cars through high-threat urban areas (HTUA).

This action is needed because PHMSA has proposed rules that would effectively contract-out to the railroad industry critical authority over public safety. That is, in the guise of requiring carriers to examine "alternative" routings of ultra-hazmat shipments, PHMSA's proposed rule would effectively shield railroads from any attempt to compel diversions.[3] In the process, railroads would enjoy the bonus of a public relations fig leaf—*non*-diversion would be seen to be compelled through the workings of a government sanctioned, black-box analysis developed, run and with results interpreted all by the very party—the affected railroad—that is meant to be governed by the outcome.[4] There would be no opportunity for the public, local government, or any other interested party to challenge the results of a PHMSA-sponsored alternative routing analysis:

> *[D]ata compiled under the proposed regulations would be considered SSI under regulations promulgated by DOT and DHS (49 CFR Parts 15 and 1520, respectively). SSI (sensitive security information) is subject to special handling rules and qualifying information is protected from public disclosure under those regulations if copies of any data are kept or maintained by DOT. See 69 FR 28066 (May 18, 2004) and 70 FR 1379 (January 7, 2005). 71 FR 76840* (December 21, 2006.

Either purposively or unwittingly, the factors proposed to evaluate alternative rail routes can only revalidate preexisting operating patterns or condemn for rank incompetence railroad management. Appropriately for a private concern but hugely inappropriate for the purposes to which they are proposed to be put, the factors most heavily weight business considerations, in passing ask about the proximity of iconic targets, and for other indicia of risk (e.g., population density) provide a countervailing factor—"emergency response capability along route" which of course correlates with population. The adequacy or inadequacy of the response capability never need be assessed, for all data and analysis performed is protected from prying eyes.

PHMSA strongly suggests that an alternative route must not only be safer and more secure than customary routes, but operating over it should not diminish profitability. Carrier decisions should be based on "the financial management principles generally applied to other business decisions." This is like mandating power utilities to provide pollution controls unless they would reduce net income or increase charges to customers. It is hard to believe that this is all meant to pass as a serious methodology applicable to any public purpose:

> *As used in this proposal, "commercially practicable" means that the route may be utilized by the railroad within the limits of the railroads particular operating constraints and, further, that the route is economically viable given the economics of the commodity, route, and customer relationship. The question of commercial practicability must be reasonably evaluated by each rail carriers a part of its analysis based on the specific circumstances of the route and proposed traffic. If using a possible alternative route would significantly increase a carrier's operating costs, as well as the costs to its customers, the carrier should document these facts units route analysis. We expect that carriers will make these decisions in good faith, using the financial management principles generally applied to their other business decisions.*

PHMSA most directly announced its abdication of authority in the NPRM to regulate routing when it noted: "[I]n promulgating its March 2003 security regulations

---

[3] Judging by news coverage, the PHMSA's proposed rules have already been positioned as "reroute friendly." For example:

The release of deadly chemicals from a rail car in a densely populated city could have catastrophic consequences, whether it's caused by a terrorist attack or a derailment.

Last week, transportation and Homeland security officials proposed ways to make it harder for terrorists to attack rail cars—and less likely that an accident would result in mass casualties.

Transportation Secretary Mary Peters wants rail companies to send poison gases, like chlorine or anhydrous ammonia, and other hazardous cargo along routes that pose the least danger for nearby residents. Access Controls and Security Systems, December 22, 2006.

[4] In case there is any doubt as to what the PHMSA analysis would yield, the agency awarded a grant to the Railroad Research Foundation to provide, as the NPRM puts it, "a formal methodology to assist the rail carriers in complying with the enhanced safety and security planning requirements of this proposed rulemaking." The Railroad Research Foundation is a creature of the railroad industry, and its president, also leads the AAR, where he has long been the a vociferous opponent of alternative routing requirements.

under Docket HM–232, PHMSA specifically required rail carriers to address en route security; however, PHMSA deliberately decided to leave the specifics of hazardous materials rail routing decisions, and other en route security matters covered by transportation security plans, to the judgment of rail carriers."[5]

For its part, Transportation Security Administration's (TSA) simultaneously-issued NPRM respecting hazmat chain-of-custody (and, more broadly, its increasingly sophisticated strategic processes) are welcome, and partially validate the appointment of a top-tier railroader as its head. However, more complete success will require a far more deft hand at labor relations than has so far been exhibited by DHS or is the norm in the railroad industry.[6]

It would be very poor timing indeed to throw away the one crude, but highly effective defense against train weaponization. Because it is now that the malefactors operating in the terrorist proving grounds of Iraq are turning their attention to the potential of chlorine.[7] Five weeks ago, on January 28, a dump truck with explosives and a chlorine tank blew up in Ramadi, killing 16. On February 20, a tanker filled with chlorine was exploded, north of Baghdad, killing nine and wounding 148, The following day in southern Baghdad a truck bomb that combined explosives with chlorine gas blew up killing at least two and injuring 32. Soon after, as reported by Reuters relying on U.S. military statements "Al Qaeda militants in Iraq were preparing to make crude chemical weapons using chlorine at a car bomb factory discovered west of Baghdad."

U.S. and Iraqi police spokesmen reportedly expressed concern that the bombers were in the early learning stages with respect to the maluse of chlorine, and technical advances were highly probable. The chlorine was largely combusted rather than dispersed, more efficient and sophisticated devices could apparently have been far more deadly. How much more deadly? The Chlorine Institute estimates a chlorine release maintaining a minimum 20 parts per million could be "immediately dangerous to life or health" (IDLH) 0.6 mile downwind in the event of a release of 150 lbs, 2.2 miles for a one ton release, and 14.8 miles downwind in the event of a 90-ton tank car rupture.[8] Since these estimates were made, the chlorine IDLH has been revised by the Federal Government downward, to 10 parts per million, expanding the recognized extent of deadly risk substantially.

The emerging threat represented by terrorist interest in chemical weaponry (the ability to cut a tank car open has already been demonstrated in southern Iraq, according to data compiled by Rand) warrants the inclusion in the Rail Security Act concrete instructions for the PHMSA and TSA. I would suggest that: within one year, no ultra-hazmat car should be permitted in any HTUA—and smaller cities as well—if:

1) the tank car is not in compliance with the most recently approved tank car specifications which will markedly decrease the risk of penetration by small arms and low-yield explosive devices,

2) the tank car's chain of custody has not been meticulously maintained to TSA requirements,

3) the operating railroad has failed any inspections in the past six months designed to monitor compliance with chain of custody requirements,

4) the originating shipper has been found out of compliance with relevant regulations over a similar period and

5) the rail corridor in the affected urban core is not protected by devices proven effective in deterring attacks or by stationed guards. Successful components of the Washington D.C. corridor's $9.6 million test project could be such qualified devices.

---

[5] 71 FR 76841 December 21, 2006.

[6] Even as TSA moves forward strategically, there have been precious few signs that it is advancing in the trenches. Homeland security will be ill-served if TSA morale, never high, engages with the acutely adversarial management-labor relations typical of railroads. (As example, the industry reached an interim agreement with seven unions last week—after 28 months of talks). The need for mandatory rerouting can be reduced only with stringent inspections and testing. This in turn requires a motivated force of inspectors. DHS management might reflect on a fundamental difference between Transportation Security Officers (TSO) and marines—marines emerge from training with intense pride in their organization and mutual respect of foot soldier and officers. The social contract between all is respected, and that contract provides for no bargaining. Such a "contract" in which mutual expectations are implicit is absent with respect to DHS employees.

[7] Parenthetically, the growing success of insurgent efforts at downing US aircraft should alert TSA to reenergize programs aimed at countering external, not just in-plane threats to aviation.

[8] Chlorine Institute Pamphlet 74, *"Estimating the Area Affected by a Chlorine Release April, 1998*

This would not be the first that regulation of railroad security has been "contracted out" to the very parties whose activities are intended to be regulated. Most of us who were involved in the District of Columbia's 2005 foray into the regulation of railroad movements (I was the District's rail expert in the ensuing litigation) knew that federal law preempted relevant local or state legislation. But we soldiered on because at the time, there was no federal law to do the preempting. The District had no choice but to defend itself, for the federal government certainly wasn't going to fight for the city. And, sure enough, the Justice Department, Homeland Security, the Surface Transportation Board—all chimed in arguing that federal law trumps.

But what was the preempting federal law? TSA, which in theory had sole jurisdiction, had not promulgated any rail security regulations; it was too involved in refighting 9/11. All there was a "top-secret" (Association of American Railroads (AAR) words) voluntary plan dashed together by the rail industry in December 2001 in a successful effort to forestall regulation by the federal agencies that were supposed to be doing the work. This law was so top secret that it could not be divulged to the District's lawyers, its lawmakers, or, from what I could discern, a Federal Judge. Of course, all railroads which interchanged with US roads necessarily participated in the planning process, so my understanding is that Canadian and Mexican nationals did receive sufficiently elevated security clearances from the AAR so that they could make a contribution. The AAR then informed anyone who would listen that the plan rated a grade of "A" from this federal agency or that military officer.

Mr. CUELLAR. [Presiding.] Thank you very much.

And I thank all the witnesses for their testimony.

I would now recognize myself for 5 minutes of questioning.

Mr. Hamberger, according to the GAO, the FIA has been focusing its efforts to improve rail safety addressing issues such as human error inspections and railroad track failure. And it seems that the industry views safety as a bigger, more pressing concern than the risk of terrorism.

I know that in part of my district in San Antonio, as you know, there have been several, several, several incidents dealing with some of the issues I just mentioned. Is there a nexus between safety and security concerns? And what measures would you recommend that have been or can be implemented that serves both purposes of safety and security?

Mr. HAMBERGER. Well, I appreciate that question, Mr. Cuellar. And I am unfortunately aware of the accidents that have occurred down in Bexar County. There is a definite overlap correlation between safety and security. And we have tried at one end of the spectrum to make sure that our employees in their daily safety briefings that Mr. Weiderhold mentioned has now been expanded to be a safety and security awareness briefing.

But in other areas, for example, I mentioned the research at the transportation technology center. We are working on a laser-based imaging machine that when a tank car would go by or any car really would go by, we would be able to see if there is something that would check against the database to see if there is something hanging or attached to that car that should not be there. And it could be a broken bar. Or it could be a trailing air hose. Or it could be something that a terrorist had planted. So there is some correlation there.

In addition, we have gone through a major effort to try to improve the crash worthiness of the tank cars that move the toxic by inhalation chlorine and the anhydrous ammonia, to name two, around the country, about 100,000 carloads a year. We came up with a new standard. It was to go into effect January 1, 2007. It

would make it both more impregnable to assault by terrorists as well as safer should an accident occur.

At the request of the Federal Railroad Administration we have deferred the implementation date of that until January 1, 2008. But there is a definite overlap between safety and security.

Mr. CUELLAR. Okay. Could I ask you if you have any other recommendations that you can provide in writing to our committee clerk?

Let me ask another question, the line of questioning I had to the prior panel. Knowing what goes through the border—I think one of the other witnesses said once it gets into the United States we know what is happening. But, you know, being from the border area, I certainly want to make sure that we look at the safety of the public and the employees, whether governmental employees or rail employees or those rail cars coming into the United States. That is, before they hit the border.

Could you tell us a little bit of any suggestions you might have? Because I know in the Laredo area they were talking about doing some inspections on the other side. And I think that hearing got postponed. I know that some of the employees or some of the unions here had concerns about that for different reasons.

But could you tell us a little bit about inspections coming in from that we might do on the other side and how we can also use technology to move those rail cars faster through those X-ray machines that we have?

Mr. HAMBERGER. Well, you hit the nail right on the head there with the X-ray machines, which are set up at all of—as I understand it, that close to 100 percent of rail cars coming into the country by land, that is to say from Canada or Mexico, go through an X-ray machine.

We need to get to the Customs and Border Patrol, I believe it is 24, it might be 48 hours in advance an electronic consist. They are then able to as the train rolls through the machine to try to match up what is on the consist with what they are seeing inside of the car.

And if there is a question or a concern, they need clarification, they notify the train engineer and it is pulled over and they inspect that car. So I am pleased to say that we are North American network. The major Canadian railroads, the major Mexican railroads are members of the A.R. and subscribe to our car tracking system. So there is a system in place for inspecting the rail cars as they come across by land.

Mr. CUELLAR. Do you feel satisfied with the integrity of the information that is given to us before it gets to the U.S. side?

Mr. HAMBERGER. I have no reason not to be satisfied. But let me do some questioning of the people who are more involved on the day to day basis and respond, if I could, for the record.

Mr. CUELLAR. All right. Thank you.

At this time, the chair will recognize other members for 5 minutes. The chair recognizes for 5 minutes the gentleman from California, Mr. Lungren.

Mr. LUNGREN. Thank you very much, Mr. Chairman.

Mr. Rodzwicz? Is that how you pronounce it, Rodzwicz? I want to pronounce it correctly.

Mr. RODZWICZ. I have been on this Earth for 60 years, and no one has ever pronounced it the first time correctly.

[Laughter.]

It is Rodzwicz.

Mr. LUNGREN. Rodzwicz.

Mr. RODZWICZ. Yes.

Mr. LUNGREN. Thank you.

Mr. RODZWICZ. Just don't look at it when you pronounce it, you will be fine.

[Laughter.]

Mr. LUNGREN. That is fine. A lot of vowels.

Mr. RODZWICZ. Yes.

Mr. LUNGREN. And a few consonants.

Mr. Rodzwicz, we have had some discussion about the background check and the limitations placed on it with respect to this bill.

Some are concerned that the language is imprecise, such that it would prohibit a rail line, a transit line from dismissing an employee for legitimate theft, a background in theft or, let's say, someone at a bus company, a DUI in the background, because it specifically limits it only to the felonies that are in here.

Number one, is that your reading of this section of the bill? And, number two, if it is, would you support us putting language in there that would make it clear that the entities would have the ability to do that so long as they were not making a claim that it was for security reasons?

Mr. RODZWICZ. Quite candidly, I would like an opportunity to review that portion of the bill more closely.

I like to be conversant with a subject before I provide an answer and I haven't had that opportunity as of yet.

Mr. LUNGREN. Well, let me put it this way. Would you have an objection of the bill specified that that section which limited the felonies for which a background check could be done and for which someone could be disabled from working were limited to the area of security?

Mr. RODZWICZ. At this point, I would say yes. But once again, I think we have to look at it perhaps on an individual basis.

One example that comes to mind, let's, for example, say that we have a young college student that was caught with some substance in his college years that might be or is a felony.

Should we hold that individual liable for something that happened, say, 30 years ago or 20 year ago? I don't know.

Mr. LUNGREN. You stated in your written testimony that there should be mandatory review and approval of all vulnerability assessments and security plans.

Let me ask you, should that be for all under all circumstances, in that this bill would include all public transportation, including a number of public transportation agencies that are no larger than a handful of employees for, for instance, paratransit buses?

In other words, should we require that of the department or only require the secretary to review those that are most serious, from his standpoint?

In other words, here we are asking the secretary to have responsibility in these areas. Should we have it in every single possible

company that might be there or should we use the risk-based approach that the secretary and his department should only be looking at those of a particular size, for instance?

Mr. RODZWICZ. I would say, at this point, yes, we should, but, however, I rely on the educated people that serve the public in Congress to make a better judgmental decision on that issue.

Mr. LUNGREN. Thank you.

Mr. Millar, do you believe and is it the position of your association that the public transportation security grants should be risk-based?

Mr. MILLAR. Yes, sir. We are fully supportive of that concept.

Mr. LUNGREN. There has been some discussion on the Hill, not yet in this committee, that we ought to have two agencies of the government handle these security grants, DOT and DHS.

What is your association's position on that?

Mr. MILLAR. Our view has been that the Department of Homeland Security has not proven itself to be a good grant-making agency and that the Department of Transportation has had relationships going back 40 years or more with the transportation systems involved.

And our view has always been that the Congress should set the policy in cooperation with DHS, but once the policy is set, once the program is established, the money should be transferred to the Department of Transportation for purely administrative purposes.

DOT is already set up with grant application processes, with audit processes, with payment processes and things that at least so far DHS has not done a good job of.

Mr. LUNGREN. But wouldn't that be an argument against us ever setting up a DHS in the first place?

That is, we tried to take responsibilities from other agencies and departments that existed for decades because the Congress believed it important to have a single department of government which, across all agencies, would be the primary instrument of the federal government with respect to security from a homeland security standing.

Mr. MILLAR. Our view has been that Department of Homeland Security, if the Congress wishes to set up such an agency to centralize the policy of the government in this regard, that is perfectly fine with us, but we think it doesn't make sense to take advantage of administrative structures that already exist across the government that work perfectly well, why duplicate those.

And in the 5 years since DHS has been created, I can tell you chapter and verse of all the different difficulties that they have had, including four times reorganizing the agencies that are responsible for these grants.

We still have members who have not been able to spend their money that you appropriated in the year 2004. It is not a system that is working well.

It may get better, but why not use a system that is working well? Keep the control, as the Congress wishes, centralized, but allow simply the administrative function to work to allow the funds to flow quickly.

Mr. LUNGREN. I thank the gentleman.

Mr. CUELLAR. Thank you, Mr. Lungren.

At this time, the chair will recognize for 5 minutes the gentleman from Massachusetts, Mr. Markey.

Mr. MARKEY. Thank you, Mr. Chairman.

Mr. Shuman, you testified in the D.C. court case on rerouting that you did not believe that CSX would incur any significant harm to its business as a result of compliance with the District of Columbia act.

Could you please elaborate on why your cost estimates were so much lower than those submitted to the court by CSX and what assumptions did CSX make that you feel were erroneous?

Mr. SHUMAN. Congressman, for starters, CSX admitted that it really did not make any cost estimates, that it was unable to, that there were too many different kinds of costs and it was a very complex process.

And so they had a back-of-the-envelope figure based upon diverting all cars that had, in the past, gone through the District of Columbia, but substantially more cars that had been going through after the voluntary diversion plan.

So their estimate of about $2 million in costs versus ours of about $800,000 really, though, reflected a different base number of cars.

Nevertheless, their $2 million estimate still was a small fraction of 1 percent of their total system revenues.

Mr. MARKEY. Mr. Hamberger, has AAR conducted its own cost-benefit analysis associated with requiring the most hazardous materials to be rerouted?

Mr. HAMBERGER. We have not.

Mr. MARKEY. You have not.

So are you in disagreement with Mr. Shuman in terms of his analysis?

Mr. HAMBERGER. I have not studied his analysis.

Mr. MARKEY. Okay, thank you.

Mr. Shuman, from your perspective, do you believe it to be minimal, the cost for rerouting the tiny percentage of extremely hazardous shipments?

Why do you think CSX has so vigorously opposed the District of Columbia act?

Mr. SHUMAN. Well, in fact, TIH or the chemicals in question total three-tenths of 1 percent of railway business and even a fraction of that was involved in HAZMAT.

I can tell you my personal conspiracy theory with respect to that and that is that the railroads resist very strongly any infringement on their sovereignty over their rights-of-way.

They have fought tooth-and-nail over competitive access. They fought very hard, made things very difficult—I am very glad to hear that Mr. Hamberger and Mr. Millar are on good terms now, but they made it very difficult for commuter systems to be developed that would operate or share rights of way with railroads, partly on safety reasons, but partly because they could extort very high dividends by selling off these rights to states when the states had no competitive alternatives.

I think that they see that as a precedent, that their backs are up because it is a slippery slope from if there is control, people

begin to tell the railroads how to do something on their right-of-way, interfere with their use, then some day they will allow—

Mr. MARKEY. You aren't saying that they oppose even homeland security mandates because they think it could lead to other things. So they have to be pure and oppose any kind of government regulations. Is that what you are saying?

Mr. SHUMAN. Absolutely.

Mr. MARKEY. Let me just stop you there.

Mr. Shuman, your testimony recommends that the committee add language to the bill that prohibits railroads from moving extremely hazardous materials through high threat urban areas.

During next week's markup of legislation, I plan to offer an amendment that will require rail carriers to analyze both the routes they use and the locations in which they store extremely hazardous materials and to require DHS to issue regulations that require the rail carriers to use the most secure routes and storage facilities so that areas of concern would be avoided whenever possible.

Is that approach consistent with what you are recommending?

Mr. SHUMAN. I am not quite as absolute as you are. I agree, in general, but I believe that if railroads can demonstrate that their operations are consistent with a number of factors, such as rigid adherence to DHS' proposed rule on chain of control, chain of custody over cars, that the tank cars are all hardened to the latest standards which came out a couple of months ago, that they have been inspected thoroughly inside of the wheel wells and the bogies and everything else, if there is no IUD, that he is there, that no one has access to the tracks in the area—

Mr. MARKEY. Let me just stop you there.

Let me go to you, Mr. Hamberger. In your testimony, you claim that you are in opposition to the banning of shipments of extremely hazardous materials.

You claim that the ban could foreclose the safest routes from being used and reduce safety as a result.

Are you saying that some rural routes are not safe enough for extremely hazardous materials to be shipped on and do you have a list of those routes?

Mr. HAMBERGER. What I am saying is that by rerouting around an urban area, you may increase the number of miles that a loaded tank car would be moving. It might move over track that is not signaled, for example.

It might go through areas where the emergency responders have not been trained as well as in the area where it currently goes.

So as I understand, for example, the voluntary rerouting that CSX is doing on its north-south line currently is adding about 2 million miles of additional travel by loaded tank cars around the country and that is 2 million miles of additional exposure.

Mr. MARKEY. And setting the safety question aside for a moment, does AAR agree that terrorists would be more likely to attempt an attack on a shipment of extremely hazardous materials if the shipment was traveling through a densely populated area rather than along a more remote route?

Mr. HAMBERGER. Mr. Markey, it is, I think, difficult, as Mr. Cuellar pointed out, to separate the safety and security items from each other.

We have absolutely no indication that there is any threat assessment that there is going to be an attack on freight rail. There has not been such an attack that we are aware of.

There are lots of attacks on passenger rail.

Mr. MARKEY. Thank you, Mr. Chairman.

Mr. CUELLAR. Thank you, Mr. Markey.

At this time, the chair will recognize for 5 minutes the gentlewoman from the District of Columbia, Ms. Norton.

Ms. NORTON. Thank you very much, Mr. Chairman.

Don't think I am not sympathetic with industry, tracks laid, they were laid 100 years ago. They are not like trucks that have some mobility.

And yet you carry the most hazardous materials in the country and you have to carry them. You are a common carrier and I understand that.

Mr. HAMBERGER. Thanks for recognizing that, yes, ma'am.

Ms. NORTON. You are a common carrier, you have got to carry them, and I just think this needs to be figured out.

I certainly don't believe that one could reroute traffic very easily or very often. The reason that the courts have sued one of your members, of course, has more to do with the regulators than it does with them, because the District, left without any action by Congress and any action by the regulators, on its own motion, said we have to do something.

Mr. Shuman, as I understand it, you were helpful to the city in this regard. The point was that even under commerce clause authority, a local jurisdiction doesn't have to sit there and be a sitting duck.

And so they tried to issue their own rerouting motion. Then, of course, rerouting is possible here. We even understand that rerouting has taken place here.

To show you the seriousness of this matter, the court, of course, still has the matter before it. So it didn't just come about because the District is a local jurisdiction.

I wasn't able to get from the last panel even the notion that notice ahead of time.

I would ask this question then of, I guess, Mr. Hamberger, any of you who are equipped to answer this question, whether you think that at least in some instances, like the nation's capital of the United States, for goodness sake, where, in fact, alternative routes, alternative tracks do exist, where you have not only the nation's capital, but 4 million people in the region, where the entirely federal presence is located, in a situation where there are, by any light, it seems to me, exceptional circumstances, where rerouting would be possible in those limited circumstances, do you think that working with the authorities, that might be a prudent thing to do?

And for places where it was not, and I am willing to concede that that is probably most places, what do you think should be done to protect local jurisdictions beyond moving trains?

I understand what has already been done. And do you believe that the notion of giving some notice that hazardous materials to

a highly placed official with the appropriate security rating might be an appropriate thing to do, to give some sense to first responders that they might want to be alert?

And if not that, what alternatives do you propose? I have named two for you and I would like to hear your response.

One, for quite exceptional jurisdictions, and, two, for most jurisdictions in the United States who might not be able to reroute and bearing in mind your own concerns and your own industry.

Mr. HAMBERGER. With respect to rerouting around the District of Columbia, the CSX did, of its own volition, in consultation with the Department of Homeland Security, post the Madrid bombing, made its own determination based on its own security plan that it would be prudent and appropriate to reroute around Washington, D.C.

Ms. NORTON. Are you testifying that CSX is rerouting around Washington whenever hazardous substances are coming through this area?

Mr. HAMBERGER. On their north-south line, that is correct. That is my understanding and that they did that of their own volition and—

Ms. NORTON. Because they have never conceded that and it is important to hear that, if that is happening.

Now, of course, you have areas like New York and God knows how many others which have even larger populations. New York happens to get more threats by far than even the nation's capital.

Mr. HAMBERGER. I think you just—

Ms. NORTON. Again, I am not trying to pin you down on jurisdictions. I am really trying to say what do we do.

Mr. HAMBERGER. I think that is really the broader question, is really the great question, and, that is, what do we do.

Ms. NORTON. And I have given you something that seems to me to be fairly mild, just to say, "Look, we are not doing anything," but for your police chief, you, TSA—maybe TSA should tell us who that should be.

But we do want you to know that—

Mr. HAMBERGER. We do indeed notify the emergency responders of the materials that are moving through there by jurisdiction to try to make—

Ms. NORTON. But not when the last panel said—the last panel said—

Mr. HAMBERGER. Not exactly when, no, ma'am. We subscribe to that theory, as well, that—

Ms. NORTON. Mr. Hamberger, let me stop you right there.

When I examined him and said I can understand your security concerns and without trying to make it worse and I named the police chief, who, certainly, in every large jurisdiction, has the appropriate security clearance, I named the fire chief, I named the two chiefs' first responders, he was not willing to concede that even they should know when hazardous substances are traveling through a local jurisdiction.

Are you sitting there and telling me that you think that is reasonable?

Mr. HAMBERGER. We are indeed telling those individuals what hazardous materials are moving through there and—

Ms. NORTON. What good does it do if they do not know when it is coming and nobody in the jurisdiction knows?

Mr. HAMBERGER. When an incident happens, we are immediately in touch with them and they—

Ms. NORTON. Sorry, sorry?

Mr. HAMBERGER. When an incident happens, we are immediately in touch with the emergency responders so that they can respond.

Ms. NORTON. Oh, my God, Mr. Hamberger, you are testifying that when an incident happens and when you are blowing up, they will tell you you are blowing up.

This committee is about prevention. After 9/11, the entire Congress has been about prevention. And all I am asking, particularly in light of my understanding of your own liabilities, of your own concerns, of the situation as an old common carrier you are in, I am simply asking you what would be the harm in telling the two chief security officers in a local jurisdiction that hazardous substances are traveling through.

By the way, they would probably be gone in 5 minutes, the way trains travel, but are traveling through and telling the time and the day they are traveling, what would be the harm to your industry in doing that?

Mr. HAMBERGER. The reason we have not required that is because it is our belief, as Secretary Hawley indicated, that that would be a potential security degradation and so we have not—we do tell the communities and it, of course, is something that our electronic consist has, as well, when there is an incident, what is in each car and what the appropriate response is.

Ms. NORTON. And you say, "And guess when it is coming." I must tell you, Mr. Hamberger, that is why there is going to be a bill here. There should have been a bill long ago particularly considering the issues raised by these substances.

And when I hear you say that, even though I have conceded to you that there may be few jurisdictions where you could reroute and have asked you, on your own motion, to come forward with what could be done concerning moving vehicles and the industry is not able to say that even notice to people with high security clearances would be appropriate, you can see why regulation is appropriate and necessary.

And I must tell you, I don't think there is a single member of Congress who would agree with you that the police chief and the fire chief should not know when hazardous substances are traveling through their jurisdiction.

I cannot think that in either party there would be anybody to come forward and show his face and raise his hand and say "amen to that."

And I thank you, Mr. Chairman.

Mr. CUELLAR. Members, at this time, we will go into a second round of questions. And at this time, I will recognize myself for just one question.

Mr. Hamberger, this has to do with the rail bridges, the crossings that we have. And, again, I have my own opinion, because I have seen the rail bridges.

Do you think there is adequate protection and security of the rail bridges? And I am talking about the international rail bridges.

And keep in mind, for example, let me give you a scenario. Let's assume something were to happen while a train would be crossing carrying certain types of hazardous materials and it would spill into the Rio Grande and think about what would happen if you have literally thousands of people on both sides of the river with that type of materials.

Do you think that there is adequate—that we need to do more to help protect the rail bridges, the international crossings that we have?

And, quite honestly, I have my own opinion, but what is your opinion of your?

Mr. HAMBERGER. Mr. Cuellar, as part of the risk assessment and vulnerability assessment that we did as an industry, we went out and we actually identified 1,308 critical assets of the rail network.

Many of those are indeed bridges and it is our view, with 140,000 miles of track in the United State alone, that it is impossible to guard every mile, every bridge at all times.

And that is why we have set up at the AAR a secret level operations center that is tied in to the national and joint Terrorism Task Force, that is tied into the intelligence center at TSA, so that if there is any credible threat, resources, our own police forces and the FBI can be directed to provide protection at that point.

And that actually is part of my written testimony, is an idea, instead of going from 100 inspectors to 600 inspectors, perhaps those additional personnel could be used in more of an air marshal kind of situation as opposed to just going out and inspecting compliance with TSA regulations.

Mr. CUELLAR. What sort of priority do you all give to international border crossings? And the reason I say that, because I am very familiar. I am an attorney, but I am a custom broker.

Mr. HAMBERGER. When we looked at—

Mr. CUELLAR. I am a custom broker, so I am familiar with movement of goods coming in and I am a big believer of trade. I think you know my record. I am a big believer in trade and I want to see those cars coming in.

But at the same time, without impeding trade and tourism, I certainly want to make sure we provide that balance of security especially for rail.

Mr. HAMBERGER. As we took a look at it, and we did this with the assistance of a consulting firm here in town who is comprised primarily of former military and civilian intelligence personnel, we asked them to come in and take a look at our system the way they would look at it if, indeed, they were looking to attack it.

They brought with them their best practices from the intelligence community and they looked at harm that could be done to the economy, harm that could be done to the population, and harm that could be done to our military preparedness and where those three circles intersected.

And then, of course, a follow-on was what kind of recovery if possible, and that is why bridges are, indeed, an issue of concern.

So I don't know whether the international aspect of that played into that analysis, per se, but, certainly, given the level of economic activity across those bridges, they certainly would have to be high on the list, I would think.

Mr. CUELLAR. All right, thank you.

At this time, Mr. Lungren, do you have any questions?

Mr. LUNGREN. Yes, thank you, Mr. Chairman.

Mr. CUELLAR. At this time, the chair will recognize for 5 minutes the gentleman from California, Mr. Lungren.

Mr. LUNGREN. Mr. Shuman, I would like to just ask you some questions about this rerouting of hazardous materials around urban areas.

How do you define urban areas?

Mr. SHUMAN. An urban area would have to be an HTUA. I am not sure precisely what the definition is. It has to do with population density. It has to do with also the urban areas that you would want to avoid, ones with iconic targets, places that, for some reason, there would be a—

Mr. LUNGREN. Let me ask you, how would you distinguish between San Francisco and Sacramento, which I represent?

Mr. SHUMAN. They are both quite populous.

Mr. LUNGREN. San Francisco is far more populous. The Bay Area is more populous than the Sacramento area.

My question is if you were to reroute it to get it out of the San Francisco area, if someone decided that was iconic, what do you say to the people of Sacramento?

What I guess I am asking is, it is not quite as easy as saying we are just going to reroute it around urban areas, is it?

Mr. SHUMAN. Well, there is a conflation between security and safety, as well as convergence.

Mr. LUNGREN. Well, I don't care about conflation and convergence.

What I am saying is, okay, we reroute it away from the capital of the United States. That is important. And I don't know where the tracks otherwise lie, but let's say it follows the path of the Beltway.

So now you have exposed the people in the surrounding area of D.C. rather than D.C. itself.

Mr. SHUMAN. You have exposed them to an increased safety risk, which is miniscule. The railroads have an exceptional safety record.

We did calculations on the CSX diversions, 2 million additional miles a year would produce a possibility of a major accident once in 1,136 years.

Mr. LUNGREN. Now, we are on security. The issue is security. If you reroute it around going directly through D.C., and I might happen to agree with that, because that is the nation's capital, but let's say that requires you to go around here.

So you go around the suburbs of D.C. You are still exposing people in those suburbs to the potential of a terrorist attack, if, in fact, their point is to attack a particularly security-sensitive material that is on that train, right?

Mr. SHUMAN. I would think that the possibilities are vanishingly small and that is because, as I noted, that I don't think there will be more than one terrorist attack on a tank car, because I think that Al Qaeda would recognize that the counterterrorist techniques that go into place after something like that happens, they won't have a crack at it again.

They are going to look for these most promising, the most biggest statement they can make and they are not going to waste it on the suburbs of Washington, D.C. or in Sacramento.

Mr. LUNGREN. They aren't, you can say that with absolute certainty.

Mr. SHUMAN. I can't say that with absolute certainty, but—

Mr. LUNGREN. Well, neither can I. So what I am trying to suggest is maybe it is a little more complicated than saying if you reroute it around urban areas, that you are ensuring that it is not going to be the subject of a terrorist attack.

I mean, look, when I was attorney general of the state of California, we had an issue about whether or not we were going to allow, by the federal government, to take spent fuel rods that were taken from foreign countries that we take into the United States and that is part of our overall obligation under the treaty to make sure of nonproliferation.

So we happen to think we trust ourselves better than we do other countries. And some local communities wanted to stop it from going through there.

If we allowed local communities to stop it from going through there, it would protect those local communities, but the damage, the danger to the rest of the world from nuclear proliferation would be greater.

The federal government, in that regard, did not allow local governments to say, "No, you can't come through our areas," number one.

Number two, as I recall, we didn't give them the time at which it came through either, because we thought that would be, at least the federal government thought, at that time, that would be of a more serious nature.

So I may disagree with Ms. Norton that maybe there are some people in the Congress who have a different opinion, which might be the more you give out information with respect to times that things may come through as opposed to notifying the communities this may come through at a time, therefore, be prepared with your response, is a rational balancing of the concerns that are out there.

And that is the only thing I would like to raise, because I have sat here and listened to presentations which suggest that there is just one way to look at it and it might be a little more complicated than that.

And while in some cases it may make good sense to reroute it around an urban area, in other circumstances, it may not.

And maybe I am not pressing enough, as some members are, to be able to know absolutely that it is perfect or it is the proper rule every time.

So I thank you, Mr. Chairman, for my 5 minutes.

Mr. CUELLAR. Thank you, Mr. Lungren.

At this time, the chair will recognize for 5 minutes the gentleman from Massachusetts, Mr. Markey.

Mr. MARKEY. Thank you, Mr. Chairman.

Mr. Hamberger, you have testified that more than 2,000 rail employees have been trained as part of an AAR program.

How many of these employees are frontline workers?

Mr. HAMBERGER. I believe, to be precise, Mr. Markey, my testimony said 20,000 emergency responders get trained by us each year around the country and we are in the process of giving a frontline—all the frontline employees security training.

Mr. MARKEY. Twenty thousand. So 20,000—

Mr. HAMBERGER. Twenty thousand emergency responders.

Mr. MARKEY. Twenty thousand rail employees—

Mr. HAMBERGER. No, sir. These are emergency responders in communities in which we operate. The rail employees—

Mr. MARKEY. How many rail employees have been trained?

Mr. HAMBERGER. Well, they are all getting security awareness training and those that whose job requires them to deal with hazardous materials receive the training under HM–232 at FEMSA. So all of those would have received the training.

Mr. MARKEY. Well, the Teamsters recently reported that approximately 90 percent of them have received no security training whatsoever.

Now, security awareness is one thing. Security training is something else. So how many have received security training?

Mr. HAMBERGER. I would submit to you, sir, that the training that we are in the process of giving to all frontline employees, and you were not here in my testimony where the TSA has done a survey of 2,600 rail employees and found that 80 percent of them had a medium or high level of security awareness.

I think our security—

Mr. MARKEY. Do you dispute the Teamsters' argument that 90 percent of them have received no security training whatsoever?

Mr. HAMBERGER. I would suggest that if they went back out in the field at this point, they would have a much different result considering—

Mr. MARKEY. And what percent do you say have received security training?

Mr. HAMBERGER. TSA found 80 percent had a medium or high level of security awareness and 100 percent will have it by the end of the year.

Mr. MARKEY. Would you provide to the committee, not TSA's, but your own documentation of the training?

Mr. HAMBERGER. Yes, sir.

Mr. MARKEY. Of workers.

Mr. HAMBERGER. Yes, sir.

Mr. MARKEY. For not awareness, but actual training.

Mr. HAMBERGER. Well, there are two different things, sir. There is the security awareness training and that is to say when someone sees something that is not normal, sees something—I have an example here of a BNSF employee who noticed that there were not any flags out as some work was being done around a railcar and that is not safe.

There should have been some blue flags out and he went and realized, as he was going to warn his fellow employees to put the blue flags out, that these weren't exactly well-meaning folks.

They were stealing things out of an intermodal van container. He called the Burlington Northern police, who came and took care of the situation.

So you recognize and report. It is our philosophy that it is not up to the individual employee to become a law enforcement officer. That is why we have law enforcement officers.

Mr. MARKEY. Let me go to Rodzwicz.

Mr. Rodzwicz, can you please comment on what you just heard from Mr. Hamberger?

Mr. HAMBERGER. Yes. If Mr. Hamberger would like to pay for another survey done by the Teamsters, I think we would be more than willing to show that security awareness and security training are two different things.

Mr. MARKEY. Could you provide to the committee your own analysis of this problem in terms of the number of Teamsters that have been trained?

Mr. RODZWICZ. Yes, I will.

Mr. MARKEY. I appreciate that very much.

So you dispute the key assertion made by Mr. Hamberger.

Mr. RODZWICZ. Unfortunately, today, my colleague and I disagree.

Mr. MARKEY. And let me ask the whole panel

Do you think that TSA should be mandating security training for all rail, mass transit employees?

Mr. MILLAR. Our view is that they should be supporting our security standard-setting program and part of that could certainly include training. But to mandate something—

Mr. MARKEY. That they could or should?

Mr. MILLAR. Excuse me?

Mr. MARKEY. Could or should?

Mr. MILLAR. That they should be supporting it, yes, sir.

Mr. MARKEY. Should. That is helpful to me.

Yes, Mr. Hamberger?

Mr. HAMBERGER. We are already providing that training and we would welcome their review and work with us on what the requirements—

Mr. MARKEY. Do you think it should be mandated?

Mr. HAMBERGER. We are already doing it, so I am not sure what it would add since we are already doing it.

Mr. MARKEY. Would you oppose if we mandated it?

Mr. HAMBERGER. No, sir.

Mr. MARKEY. Mr. Rodzwicz:

Mr. RODZWICZ. No, I would not.

Mr. MARKEY. Okay, great.

Mr. Weiderhold?

Mr. WEIDERHOLD. I think it should be mandated. Security awareness and security training go hand-in-glove. You need a building block first. Then you need to customize the training for the craft of employees.

That is taking place at Amtrak. I am sure it is taking place at other roads right now. It is an iterative process.

Mr. MARKEY. Thank you.

Mr. Shuman?

Mr. SHUMAN. I believe that every railroad employee should be taught to be aware of suspicious events.

However, I believe that some of the problems that you have seen in rail yards of not confronting interlopers, where some of the risks

are very high, is a result of not wanting to face somebody with a knife or a gun there.

If I were a railroad employee—

Mr. MARKEY. I appreciate that. I am not asking you that question. I am asking you the question of should there be mandated security training.

Mr. SHUMAN. Every railroad employee should be made aware and if that involves training, absolutely.

Mr. MARKEY. Okay, fine. I understand there are complications subsequent to that, but that is the key question I wanted to ask.

Thank you, Mr. Chairman, very much.

Mr. CUELLAR. Thank you, Mr. Markey, for your questions.

I believe we have gone now through the first and second rounds of questioning.

At this time, we have also received statements for the record from representatives of the Citizens for Rail Safety and the American Bus Association. I ask for unanimous consent that those statements be included in the record, without objection.

[The information follows:]

FOR THE RECORD

PREPARED STATEMENT OF PATRICIA ABBATE, EXECUTIVE DIRECTOR, CITIZENS FOR RAIL SAFETY, INC.

Mr. Chairman, Congressman King and Members of the Committee, I am pleased to submit this statement before the Committee on Homeland Security to address important issues relating to the safety and security of our rail system.

Citizens for Rail Safety is a public advocacy non-profit public interest group dedicated to improving rail safety throughout the United States. We are actively engaged in providing proprietary academic research regarding a broad spectrum of freight and passenger rail issues in the fields of safety and security.

On any given day, thousands of trains move across the American landscape. Each one of them presents a potential threat to the safety of individuals and families, to the continued functioning of our communities and our economy, and to the life of our great cities. Whether carrying millions of workers to and from their jobs, or providing the safest means of transporting hazardous materials, or bringing food and agricultural necessities to consumers, railroads pose an inviting target to would-be terrorists, along with the ever-present risk of an unforeseen accident or derailment.

As most of us here are already aware, just one 90-ton car of chlorine, whether involved in an accident or an act of terrorism, could create a toxic cloud 40 miles long and 10 miles wide and could kill as many at 100,000 people in 30 minutes, if its contents are released.

Between 1988 and 2003 there were 181 acts of terror, worldwide, involving railroads and related rail targets. Security experts and government officials, as well as chemical and rail trade associations, acknowledge the vulnerability of railcars, bridges, and tunnels to intentional acts of terror. The risk of death and serious illness from unintentional accidents involving hazardous materials is also high. Though the vast majority, 99.98 percent according to the railroads, of Hazmat shipments arrive safely without major incident, there are fatalities, hospitalizations, and/or evacuations every year from the escape of a large quantity of toxic gases or liquids.

A recent study we commissioned, researched by experts at the National Labor College, found that our nation is not adequately prepared for an act of terrorism or other accidents or emergencies involving the release of hazardous materials from rail cars.

We announced the findings and recommendations of this study, *Training in Hazmat and Rail Security: Current Status and Future Needs of Rail Workers and Community Members,* at our National Rail Safety Symposium last November. During this event, we were very fortunate to have Chairman Thompson and Congressman Stephen Lynch present key notes to our audience on this subject.

Some of the key findings of this study include the following:

- Rail workers and emergency responders are not prepared for a Hazmat event. They are poorly trained in recognizing and responding to Hazmats.
- Citizens in areas of high amounts of track are uninformed about what is traveling through their cities and towns, and many do not have emergency action plans in place if a derailment or rail-related terrorist attack was to take place.
- Tracks, Cars, and Rail yards need to be more secure and protected which means the railroads need more security training for rail workers and more rail police officers.
- Radioactive waste transported with the use of the rails will increasingly grow for years, however the amount of training for communities and rail workers has remained minimal and stagnant.

Quality training for rail workers, emergency responders, and residents of rail communities—including joint training exercises—is one necessary part of an overall safety and security action plan. Changes also need to be made in rail equipment and operations to make Hazmat transport safer. With more than one million tons of hazardous materials being moved across our country each day, the need for this kind of specialized training is clear.

In two recent and fatal rail Hazmat accidents, more and better training could have saved lives. In Graniteville, South Carolina in 2005, a conductor lived because his military training taught him not to run, but to walk out of a cloud of chemical gas. Chlorine killed his engineer partner, who without training, ran and because of his deep inhalation of chlorine gas, ran to his death. Also, in Graniteville, residents did not generally know that the gas cloud that threatened them was heavier than air and that their safest escape was not only upwind, but also uphill.

In Bexar County, Texas, in 2004, three people—a trainman and two community residents—died as a result of a major chlorine leak following a derailment. If emergency dispatchers knew the dangers of rail Hazmat and the lethal nature of chemical releases, appropriate advice and a proper response to the 911 calls might have saved those residents. Instead they heard the word "smoke" and the phrase "difficulty breathing" and sent firefighters to an assumed medical emergency.

Citizens for Rail Safety is about to release the findings and recommendations from another just-completed study by Penn State University, *Securing and Protecting America's Railroad System.* This study found that resources currently directed to rail security are inadequate, given the potential for catastrophic loss of life or economic disruption from attacks on the rail system. The growing use of rail systems for work-related passenger travel and the critical role played by freight railroads in U.S. and global commerce makes insuring their security a matter of urgent public concern. While the efforts to secure the system led by the Department of Homeland Security represent a good start in tackling the issues, legislation specifically dealing with rail security is needed to identify the threats, clarify the roles of the various public and private sectors, and establish a level of funding commensurate with the importance of the rail system and the potential loss of life and economic damage that might result from terrorist attacks.

In addition to prevention, the rail system plays or can play an important role in mitigation and recovery efforts after man-made or natural disasters.

The top key findings of this study include the following:

- Across the globe, railroads have been among the most common targets of terrorist attack, leading to significant loss of life, interruption of vital services, and political repercussions.
- The rail sector in the U. S. has not received adequate resources and attention to protect it and the public from terrorist acts directed against rail operations, facilities, and assets.
- Traditional approaches to rail security, focusing on policing and cordoning of rail assets, are inadequate to provide security against post-9/11 terrorist threats. The North American rail network is too vast and diverse to be protected simply through more policing, surveillance, or anti-trespass measures.
- Responsibilities for rail security remain divided among a number of federal agencies; between federal and state agencies; between government and the private sector; and between shippers, users, and providers.
- Rail security encompasses a variety of separate threats, due to the diversity of rail operations and the still emerging nature of terrorist activities and goals.

This study identified many action steps and a list of recommendations. Some of the key recommendations from this study include the following:

- Congress needs to pass comprehensive rail security legislation and allocate adequate financial and administrative resources to enhance current security efforts.

• Resources to enhance security must be adequate to deal with potential problems and be allocated according to a careful assessment of risk, not formulas based on population or political earmarking.
• Passenger and transit operations in major urban areas, in particular those that have been targets of past terrorist acts, should receive increased percentages of all funds expended for rail security, until such time as actual terrorist acts cause a shift in the assessment of risk.
• A congressionally established National Commission on Rail Security composed of leaders from government, the rail industry, rail unions, and public representatives should be created and empowered to study the state of rail security and report back to Congress its findings within a reasonable period of time.
• Federally funded research on rail security issues should be expanded. Research should be directed both to areas of product and service delivery and scenarios that examine the consequences of possible terrorist acts against railroads.
• Information sharing within the rail security network should be enhanced through public and private investment in shared and secure information systems.
• The General Accountability Office (GAO) of the federal government should provide regular assessments of the state of rail freight and passenger security for the scrutiny of Congress, concerned government agencies, the rail industry, and the public.
• Research should be funded to examine the potential of special rail passenger operations in recovery operations after natural and man-made disasters, such as hurricanes or the release of hazardous materials in large cities. Rail has the potential to move large numbers of people away from disasters more efficiently and with a greater concern for social equity than reliance upon cars.
• Enhanced training of rail personnel to deal with both the prevention of terrorism and its aftermath is necessary, and should be a shared public and private responsibility.

As we continue to commission and release the findings and recommendations of academic studies on the topics of rail safety and security, we are also planning to take the information from these studies "on the road" this year. We will be conducting a series of "town meetings" in targeted rail communities, where we will bring together citizens, local political leaders and members of the rail community to openly discuss findings and recommendations from our studies. These meetings will bring an increased level of awareness to the residents living in areas where rail activity is high as to not only the threats inherent in our rail system, but also to the actions that can be taken to reduce those risks.

The protection of rail and public transportation systems in our country is of vital importance. The members and Board of Directors of Citizens for Rail Safety applaud the efforts of this Committee in the creation of the "Rail and Public Transportation Security Act of 2007" that has outlined a variety of actions to bring about a safer and more secure rail system.

For far too long the security and safety of our freight and passenger rail systems have been overlooked. We are encouraged that this new legislation will begin the process of securing our nation's vast rail system and we look forward to working with you on this endeavor.

Mr. CUELLAR. I want to thank the witnesses, all of you, for being here, for your valuable testimony, for your time for answering our questions, and, of course, the members for the questions that have been asked.

The members of the committee may have additional questions for the witnesses, and we ask that you respond expeditiously in writing to those questions.

Hearing no further business, the committee stands adjourned.

[Whereupon, at 1:11 p.m., the committee was adjourned.]

VerDate Nov 24 2008 14:16 May 21, 2009 Jkt 000000 PO 00000 Frm 00112 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-12\35271.TXT HSEC PsN: DIANE

FOR THE RECORD

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, A REPRESENTIVE IN CONGRESS FROM THE STATE OF TEXAS

Over the past month, this Committee has heard testimony on the important issue of rail, mass transportation, and over-the-road bus security. After hearing the experts' testimony, I, like many Americans, continue to be shocked at the lack of attention and oversight in transportation security—specifically, in the areas of rail and mass transit. I know there are many priorities this Congress faces, but I believe that in light of the horrid events of 9/11, Madrid, London, and Mumbai that we must do something to secure our transportation systems—it is with that conviction that I seek to address these issues. The recent world events are a wake-up call that we must do more to secure our transportation systems, and we must act quickly and responsibly. I firmly believe that this legislation will take an important step in securing our transportation systems.

As far back as 1995 in Hyder, Arizona, we have seen how terrorist acts severely impact our economy and transportation systems. In the 9/11 attacks, two of New York City's busiest transit stations were lost and considerable damage occurred to the tunnel structures, endangering hundreds of lives underground. This damage was so great that in the immediate aftermath of 9/11, Congress appropriated $1.8 billion to rebuild subway infrastructure that was damaged in the attacks.

Ultimately, making this bill into law takes a step forward towards protecting the more than 11.3 million passengers in 35 metropolitan areas and 22 states who use commuter, heavy, or light rail each weekday.

The RAND Corporation database of worldwide terrorist incidents, between 1995 and June 2005 indicated that there were over 250 terrorist attacks worldwide against rail targets, resulting in almost 900 deaths and over 6,000 injuries. These numbers do not include those killed or injured in the London and Mumbai attacks in 2005 and 2006.

Despite all of these attacks, rail and public transportation security *remains* secondary to aviation. The time has come for this Committee and this Congress to let the American people know where we stand on the issue of rail and mass transit security. The question for us to resolve is simple—Do we *truly* believe that it is acceptable to spend approximately 1 penny on rail security compared to 9 dollars spent on air security? For me, the answer is clear and by voting to pass this bill, I want everyone to know that we are taking serious steps to advance rail and mass transit security.

This bill authorizes more than $5.1 billion dollars for the next four years, for rail, mass transit, and bus security. With this bill—for the first time—we will have comprehensive vulnerability assessments and security plans for rail, mass transit and buses.

Most importantly, this bill finally does something to help our frontline workers, who have been left out in the cold when it comes to security training. Labor organizations have repeatedly called for additional training for rail and mass transit employees. The absence of mandated security training stands in stark contrast to other transportation sectors in the United States, such as the maritime sector, and that conducted by other countries, such as the United Kingdom.

For example, shortly after 9/11, the Amalgamated Transit Union (ATU) conducted a survey of its members and found that *80%* reported that their employers had not provided them with any security training. In a subsequent survey in the fall of 2005, approximately 60% of ATU members had still not received training in emergency preparedness and response.

This bill provides the framework by which to create an ongoing and constant oversight process for transportation security. Working with other federal government agencies, the Department of Homeland Security will monitor and assess the progress made by transportation providers and their workforces. Lastly, this bill will

finally authorize some much needed human resources to the Transportation Security Administration in the form of 600 additional rail security officers.

I want to thank my colleagues for all of their hard work and dedication to these important issues, and I look forward to the witnesses' testimony.

APPENDIXES

Appendix 1: Railroad Security Research and Development Program

Freight and passenger railroad security would be enhanced if funding were provided for research and development and other projects, including the following:

- *Automated inspections of rail cars*—Build on existing "machine vision" and other technologies to develop tools to identify unknown objects (*e.g.,* explosive devices) and substances (*e.g.,* chemical or radioactive agents) on freight and passenger rail cars.
- *Communications-based train control*—Further enhance train control systems to protect passengers, trains, and/or hazardous cargo from unsafe use.
- *Emergency bridge replacement*—Test and develop ways to rapidly replace large railroad bridges damaged by terrorist acts in order to maintain the fluidity of the rail network, minimize economic disruptions, and enhance mobility.
- *Sealing rail cars*—Develop technologies to automatically seal leaks or breaches on railroad tank cars.
- *Tampering resistance and detection*—Test and develop ways to increase the resistance of critical rail infrastructure and equipment to tampering and identify track and equipment that has been subject to tampering efforts.
- *Right-of-way integrity monitoring*—Develop a comprehensive system to ensure that railroad rights-of-way are unobstructed and intact prior to the approach of a train, especially on routes with high-density passenger operations or hazmat movements.
- *Bridge and tunnel inspections*—Develop infrared, machine vision, or other technologies to automatically monitor the integrity of bridges and tunnels and the presence of unauthorized personnel and equipment.
- *Signal system security at turnouts*—Test and develop ways to verify that rail switches and turnouts are properly set and secure.
- *Computer security*—develop new technical standards governing security for railroad computer systems and ways to mitigate damages in the event of a cyber attack. The logical focal point of this R&D effort would be Railinc, a subsidiary of the AAR located in Cary, North Carolina, that focuses on rail-related information technology.
- *National transportation security research consortium*—Create a steering committee of government and industry security and operations experts to evaluate proposed projects and technologies related to rail security and identify those with the most promise. TTCI could act as program manager for such an endeavor.
- *National railroad emergency operations center*—Develop a single database and location from which all emergency responders could receive information vital. Currently, such information must be obtained from several different sources.
- *Rail infrastructure test and training facility*—Create a new facility at TTCI that includes mock-ups of bridges, tunnels, and underground stations, to simulate responses to fires, noxious gases, explosions, and other incidents, and to test new technologies for detection, containment, and treatments.

Appendix 2: Hazardous Materials Movements by Rail

Each year, 1.7 to 1.8 million carloads of hazardous materials (hazmat) are transported by rail in the United States, with two-thirds moving in tank cars. "Toxic inhalation hazards" (TIH)—gases or liquids, such as chlorine and anhydrous ammonia, that are especially hazardous if released—are a subset of hazardous materials and are a major (though not exclusive) focus of hazmat-related rail safety efforts. In each of the past couple of years, railroads have transported just over 100,000 carloads of TIH, virtually all in tank cars.

Railroads recognize and deeply regret the occurrence of a few tragic accidents involving hazardous materials over the past couple of years. Nevertheless, the rail hazmat safety record is extremely favorable. In 2005, 99.997 percent of rail hazmat shipments reached their final destination without a release caused by an accident. Railroads reduced hazmat accident rates by 86 percent from 1980 through 2005.

Still, no one disputes that efforts should be made to increase hazmat safety and security where practical. Railroads understand this better than anyone. Today, the federal government, through the railroads' common carrier obligation, requires railroads to transport these materials, whether railroads want to or not. And while accidents involving highly-hazardous materials on railroads are exceedingly rare, history demonstrates that railroads can suffer multi-billion dollar judgments, even for accidents where no one gets hurt and the railroads do nothing wrong. In essence, the transport of highly-hazardous materials is a "bet the business" public service that the government makes railroads perform.

Railroads face these huge risks for a tiny fraction of their business. In 2005, railroads moved just over 100,000 TIH carloads and nearly 37 million total carloads. Thus, shipments of TIH constituted only about 0.3 percent of all rail carloads. The revenue that highly-hazardous materials generate does not come close to covering the potential liability to railroads associated with this traffic. Moreover, the insurance industry is unwilling to fully insure railroads against the multi-billion dollar risks associated with highly-hazardous shipments. And even though TIH accounts for a tiny fraction of rail carloads, it contributes approximately 50 percent to the rapidly-rising overall cost of railroad insurance.

For all these reasons, the current environment for the rail transportation of highly-hazardous materials, especially TIH, is untenable. This leads to our recommendation that Congress should limit railroads' liability for carrying hazardous materials, perhaps modeled after the Price-Anderson Act.

In the meantime, railroads support prompt, bold actions by all stakeholders to reduce the risks associated with hazmat transport. Railroads themselves are taking the lead:

- *In December 2006, an industry committee approved a new standard for chlorine and anhydrous ammonia tank cars that will significantly reduce the risk of a release. (Anhydrous ammonia and chlorine combined account for around 80 percent of rail TIH movements.) The standard will be phased in beginning in 2008.*[3]
- *As noted earlier, railroads help communities develop and evaluate emergency response plans; provide training for more than 20,000 emergency responders each year through their own efforts and the Transportation Community Awareness and Emergency Response Program (TRANSCAER); and support Operation Respond, a nonprofit institute that develops technological tools and training for emergency response professionals.*
- *Railroads work closely with chemical manufacturers in the Chemical Transportation Emergency Center (Chemtrec), a 24/7 resource that coordinates and communicates critical information for use by emergency responders in mitigating hazmat incidents.*
- *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 helps responders prioritize emergency response plans.*

[3] The delay in implementation is due to an FRA request.

• *For trains and routes carrying a substantial amount of highly-hazardous materials, railroads utilize special operating procedures to enhance safety.*
• *Railroads participate in a variety of R&D efforts to enhance tank car and hazmat safety. For example, the Tank Car Safety Research and Test Project (which is funded by railroads, tank car builders, and tank car owners) analyzes accidents involving tank cars to help identify the causes of tank car releases and prevent future occurrences.*
• *In addition to implementing their Terrorism Risk Analysis and Security Management Plan, railroads are working with DHS and the DOT to identify opportunities to reduce exposure to terrorism on rail property.*
• *Railroads offer hazmat awareness training to all employees who are involved in hazmat transportation. Employees responsible for emergency hazmat response efforts receive far more in-depth training.*
• *Railroads are pursuing a variety of technological advancements to enhance rail safety, including hazmat safety.*
• *Railroads are working with TIH manufacturers, consumers, and the government to explore the use of coordinated routing arrangements to reduce the mileage and time in transit of TIH movements.*

Manufacturers and consumers of hazardous materials should take a number of steps to help ensure hazmat safety.

First, concerted efforts should be made to encourage development and utilization of "inherently safer technologies," which involve the substitution of less-hazardous materials for highly-hazardous materials, especially TIH, in manufacturing and other processes. As noted in a recent report by the National Research Council (part of the National Academy of Sciences), "the most desirable solution to preventing chemical releases is to reduce or eliminate the hazard where possible, not to control it." Ways this can be achieved include "modifying processes where possible to minimize the amount of hazardous material used" and "[replacing] a hazardous substance with a less hazardous substitute."[4] In a similar vein, in a January 2006 report, the Government Accountability Office (GAO) recommended that the Department of Homeland Security "work with EPA to study the advantages and disadvantages of substituting safer chemicals and processes at some chemical facilities."[5]

One real-world example of product substitution occurred at the Blue Plains wastewater treatment facility just a few miles from the U.S. Capitol. Like many wastewater treatment facilities, Blue Plains used chlorine to disinfect water. Not long after 9/11, the facility switched to sodium hypochlorite, a safer alternative.

Railroads recognize that the use of TIH cannot be immediately halted. However, over the medium to long term, product substitution would go a long way in reducing hazmat risks.

Second, manufacturers and receivers of TIH, in conjunction with railroads and the federal government, should continue to explore the use of "coordination projects" to allow TIH consumers to source their needs from closer suppliers. For manufacturers and users, this could involve "swaps." For example, if a chlorine user contracts with a chlorine supplier located 600 miles away, but another supplier is located 300 miles away, the supplier located 600 miles away might agree to allow the closer shipper to supply the user.

Third, hazmat consumers and manufacturers should support efforts aimed at increasing tank car safety and reliability. Recently, for example, the FRA, Dow Chemical, Union Pacific, and the Union Tank Car Company announced a collaborative partnership to design and implement a next-generation railroad tank car. (TTCI has been selected to support testing and developments initiatives related to this project.)

The government too has a key role to play. First, if the government requires railroads to transport highly-hazardous materials (via their common carrier obligation), it must address the "bet the company" risk this obligation forces railroads to assume.

Second, the government should help facilitate the "coordinated routing arrangements" and "coordination projects" mentioned earlier.

Third, the government should encourage the rapid development and use of "inherently safer technologies" to replace TIH and other highly-hazardous materials.

Fourth, the government should reject proposals that would allow state or local authorities to ban hazmat movements through their jurisdictions. Bans would not eliminate risks. Instead, bans would shift risks from one place to another and from one population to another. In doing so, bans could foreclose routes that are optimal

---

[4] *Terrorism and the Chemical Infrastructure: Protecting People and Reducing Vulnerabilities,* National Research Council—Board on Chemical Sciences and Technology, May 2006, p. 106.

[5] *Homeland Security: DHS is Taking Steps to Enhance Security at Chemical Facilities, but Additional Authority is Needed,* Government Accountability Office, January 2006, p. 7.

in terms of overall safety, security, and efficiency and force railroads to use less direct, less safe routes. The result would likely be an *increase* in exposure to hazmat release and reduced safety and security.[6]

If hazmat transport were banned in one jurisdiction, other jurisdictions would want to follow suit. Already, numerous cities across the country are considering hazmat bans. An integrated, effective national network requires uniform standards that apply nationwide. If policymakers determine that hazmat movements should be banned, they should be banned nationwide, not locality-by-locality.

Finally, the government should reject proposals that would force railroads to provide local authorities advance notification of hazmat movements through their jurisdictions because hazmat prenotification would not accomplish the goals of those seeking it. Upon request, railroads already notify communities of, at a minimum, the top 25 hazardous commodities likely to be transported through their area. Railroads also provide training for hazmat emergency responders in many of the communities they serve, and already have procedures in place to assist local authorities if a hazmat incident occurs. Thus, information obtained by local authorities through a pre-notification system would not improve their ability to respond to hazmat incidents in any meaningful way.

Moreover, at any one time, thousands of carloads of hazmat 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 prenotification 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.

In the event of a hazmat incident, train consists are available to emergency responders, and railroads, at TSA request, have agreed to provide movement data on all TIH cars.

Finally, pre-notification would vastly increase the accessibility of hazmat location information. Making this information more accessible could increase vulnerability to terrorist attack by magnifying the possibility that the information could fall into the wrong hands.

[6] It has been estimated, for example, that a ban on hazmat transport through the District of Columbia would result in some 2 million additional hazmat car-miles as carriers had to use circuitous alternative routes.

Appendix 3: Legislative and Regulatory Requirements and Recommended "Best Practices" Related to Homeland Security That Directly or Indirectly Call for Criminal Background Checks for Persons With Access to Railroad Property

• On June 23, 2006, DHS and DOT released their *Recommended Security Action Items for the Rail Transportation of Toxic Inhalation Hazard Materials.* "Establishing procedures for background checks and safety and security training for contractor employees with unmonitored access to company-designated critical infrastructure" was one of the recommended voluntary best practices for the rail industry in this report. On February 12, 2007, DHS and DOT released a supplement that affirmed this guidance.

• DOT regulations (Title 49, Part 1572) require that employees who perform locomotive servicing or track maintenance and are required to operate motor vehicles that contain a certain minimum amount of hazardous materials must have a hazardous materials endorsement (HME) on their commercial driver's license. To obtain an HME, a criminal background check must be performed.

• Railroad employees who require access to port facilities are required to hold transportation worker identification credentials (TWIC), a credentialing process required by DHS. Eventually, DHS plans to require a TWIC card for all transportation workers, including contractors, whose job may require unescorted access to a secure area or transportation industry. TWIC credentialing includes a criminal background check.

• The Customs-Trade Partnership Against Terrorism (C–TPAT) program, a part of the SAFE Ports of 2006 Act that was signed into law in October 2006, is a voluntary government-business initiative to strengthen and improve overall international supply chain and U.S. border security. C–TPAT gives strong emphasis to background checks for rail employees, contractors, and others who have access to rail facilities.

> Under C–TPAT's minimum security criteria for railroads, "background checks and investigations shall be conducted for current and prospective employees as appropriate and as required by foreign, federal, state and local regulations. . . .Once employed, periodic checks and reinvestigations should be performed based on cause and/or the sensitivity of the employee's position." Rail carriers "should strongly encourage that contract service providers and shippers commit to C–TPAT security recommendations." Moreover, the Supply Chain Security Best Practices states that "Temporary employees, vendors, and contractors. . .are subject to the same background investigations required of the Company's permanent employees."

• Regulations governing the transport of hazardous materials (49 CFR, Part 172.802) require carriers of certain hazardous materials to develop and implement security plans. These plans must address personnel security by implementing measures to confirm information provided by job applicants for positions that involve access to and handling of hazardous materials covered by the security plan.

Appendix 4: The E-RailSafe Appeals Process

The e-RailSafe program is an initiative developed by the Class I freight railroads to safeguard railroad personnel, assets and customer shipments. The program was developed by U.S. and Canadian railroads in partnership with e-Verifile.com, Inc. Railroads electing to use e-RailSafe are requiring contractors doing or seeking to do business with them to obtain credentials for their employees through the e-RailSafe program, a web-based service at www.erailsafe.com. The program provides testing, background checks, and badges for current contractor employees and future applicants. The website provides answers to frequently asked questions and will soon include a description of the appeals process.

Enrolling in e-RailSafe

Contractors log into the website and input basic information into the e-RailSafe system about the employees they wish to be issued credentials for work on railroad property. When the applicant completes his or her log on, a nationwide background investigation is triggered. While not all railroads use the same criteria, in general an applicant can be denied access to railroad property if he or she has had a felony conviction within the last seven years or has been in prison within the last five years on a felony conviction. A history of misdemeanors for crimes of concern may also trigger a denial of property access. After the investigation is complete, the applicant is approved or denied access onto railroad property. If approved, a credential is sent to the contractor to disburse to his or her employee.

Applicants Denied Access to Railroad Property

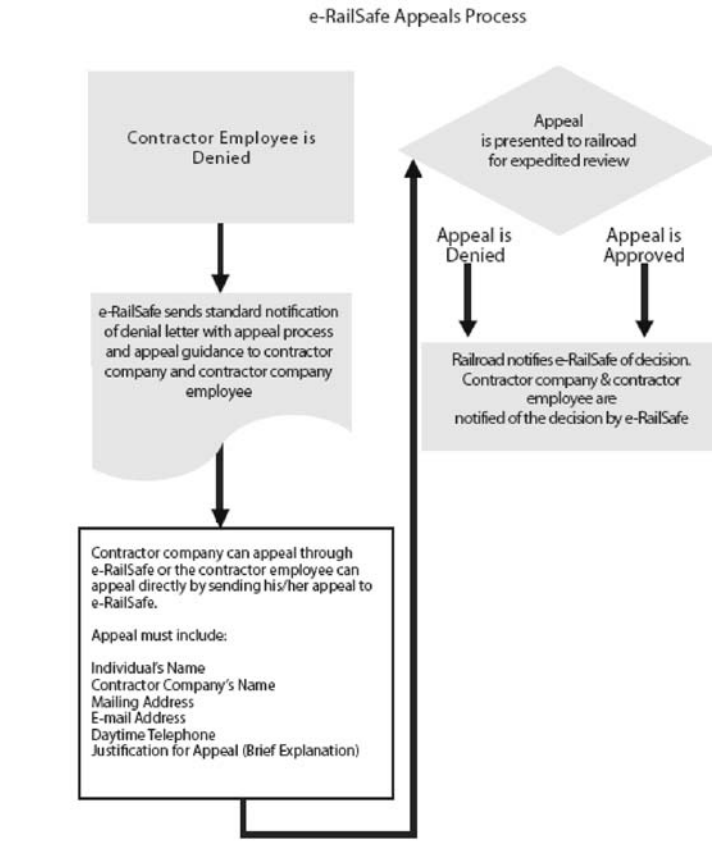
An applicant denied access to railroad property through the e-RailSafe credentialing program will be directly informed of the decision by correspondence from e-RailSafe. That letter will also include a description of the appeals process available to the applicant. E-RailSafe will also inform the applicant?s employer that credentials have been denied to the applicant and provide appeal guidance to the contractor. Both the contractor company and the contractor employee can appeal directly to e-RailSafe.

An applicant will have 15 working days from the date posted on the letter received from e-RailSafe to appeal the decision. If the applicant requires additional time to gather documentation, the applicant can notify e-RailSafe of his or her intention to appeal and is afforded an additional 15 working days to submit his or her appeal and supporting documentation. The appeal should include the following:

- Individual's name
- Contractor company's name
- Mailing address
- E-Mail address
- Daytime telephone
- Justification for Appeal (brief explanation)

Once e-RailSafe receives the appeal and supporting documentation, e-RailSafe must forward the applicant?s appeal to the appropriate railroad within 24 hours for expedited review.

The railroad must render a decision on the appeal no later than 10 working days from the date of receipt from e-RailSafe of the applicant?s appeal. The appeals boards within each railroad will include at a minimum a person from the railroad police, human resources and legal departments. The decision on the appeal will be communicated back to e-RailSafe by the railroad. E-RailSafe will promptly notify the applicant as well as the applicant's employer of the decision on the appeal.



Association of American Railroads

Appendix 5: Questions and Responses

SUBMITTED ON BEHALF OF THE ASSOCIATION OF AMERICAN RAILROAD BY EDWARD R. HAMBERGER IN RESPONSE TO HON. BENNIE G. THOMPSON QUESTIONS

Question 1.: Your industry has continuously resisted mandatory security plans and vulnerability assessments, which will be required by this legislation. However, ports, the chemical industry, and the aviation industry all have to submit mandatory plans to DHS. **Why do you feel your industry should be excluded from this requirement?**

The Association of American Railroads does not object to the federal government requiring railroads to develop and implement security plans based upon risk assessments. Indeed, railroads have already met this requirement. Railroads implemented security plans based upon risk assessments in 2001 and continue to review and refine their plans. However, the industry prefers an iterative federal review process rather than an approval process which is not sufficiently flexible to accommodate rapid changes in the security environment.

Question 2.: According to the GAO, the FRA has been focusing its efforts to improve rail safety, addressing issues such as human error, inspections, and rail track failure. It seems that the industry views safety as a bigger, more pressing concern than the risk of terrorism. **Is there a nexus between safety and security concerns? Where do those issues overlap and where do they diverge?**

The AAR does not believe that the rail industry's (or, for that matter, the FRA's) efforts to enhance rail safety in any way detract from rail security. On the contrary, safety and security for railroads are interconnected: a safer workplace will tend to be a more secure workplace, and a more secure workplace will tend to be a safer workplace.

Rail safety is constantly improving. In fact, based on preliminary data, 2006 was the safest year ever for railroads by the most important rail safety measures. Railroads are justifiably proud of this accomplishment and will continue to try to make their operations even safer in the years ahead.

At the same time, rail security is constantly improving too. The AAR's testimony recounted many of the huge variety of actions the industry and individual railroads have taken to raise the baseline of railroad security—actions that were taken without waiting for legislation or a regulatory regime to tell them to do so.

For both agencies to function effectively there must be a clear understanding of the proper roles of the FRA and the TSA. Railroads are comfortable that a proper understanding has been reached, and are committed to work with each agency and with other appropriate parties to ensure that rail safety *and* security continue to improve.

Question 3.: What measures have been or can be implemented that serves both purposes of safety and security?

Examples of measures that serve both safety and security include the use of railroad police, workforce training and inspections of track, tunnels and bridges.

Question 4.: How have you determined the greatest risk of attack for your system? What is the greatest risk?

In 2001, AAR brought together more than 150 railroad and counterterrorism experts to perform a comprehensive risk analysis of freight railroad operations. The experts identified critical assets (both physical and IT), vulnerabilities, potential consequences of an attack, and the general terrorist threat based upon known terrorist objectives, capabilities and tactics. Since that time, the Department of Homeland Security has not provided AAR with intelligence information that is contrary to the industry's risk analyses and planning assumptions. For example, there has never been a terrorist attack on freight railroads in the United States or in any other country. AAR continues to watch terrorist activities worldwide and is available 24x7 to DHS officials in the event DHS receives information that might indicate a threat to freight or passenger railroads. AAR offers to brief the Committee more fully in closed session.

Question 5.: Given the open nature of passenger rail systems—multiple access points, large crowds of people, and no barriers—can anything be done to protect these systems?

Securing rail passenger systems is a formidable task. AAR member passenger railroads have developed security systems that include multiple layers of defense, including passenger awareness campaigns, police force presence, and use of canine teams. With greater resources, passenger operators can increase police and canine forces in stations, passenger waiting areas, and on train cars. The American Public Transportation Association, representing public transit and commuter rail, has testified on this subject.

Question 6.: The Port Authority of New York and New Jersey released a report recently that the PATH train tunnels that run under the Hudson River are more susceptible to attack than previously thought. **What steps are being taken to ensure the security of the tunnels in New York and elsewhere?**

The Association of American Railroads does not represent the owners of the PATH train tunnels under the Hudson River. This question should be posed to the Port Authority of New York/New Jersey and APTA. The safety and security of tunnels on Amtrak's Northeast Corridor have long received the attention of the railroad and.federal authorities. Numerous Congressional hearings over the years have elicited detailed testimony as to the problems and solutions. Improvements using federal dollars continue to be made for the protection of the traveling public. The freight railroads have an extensive inspection program for tunnels and bridges.

Question 7.: How much money will it cost to ensure that these tunnels are secure and who should pay for these security upgrades?

The Association of merican Railroads is not in a position to answer this question. The Class 1member freight railroads of the Association of American Railroads pay for their own security upgrades as part of their operating costs.

Question 8.: It has been noted that there are far too few federal inspectors to cover the 230,000 miles of track in this country.

In addition to the continuous inspections undertaken by the freight industry itself, there are approximately 400 railroad safety inspectors employed by the Federal Railroad Administration and an additional 160 railroad safety inspectors employed by the states. These 560 inspectors examine some 219,000 miles of track on a regular basis. Using a comparison of the safety inspections for the railroad industry (FRA) and the federal safety inspections of the manufacturing industry as a whole by OSHA, there is clearly a much stronger record of inspections in the railroad industry than elsewhere. Comparing FRA inspections to OSHA inspections, there are 4,113 inspections per 1000 employees in the railroad industry versus 0.34 inspections per 1000 employees in general manufacturing. In the railroad environment, there are 2.38 federal safety inspectors per 1000 employees versus 0.02 federal safety inspectors per 1000 employees in the general manufacturing sector. Given the extraordinary safety record of the railroad industry—with last year being the safest year on record—we do not agree with the notion that there are insufficient numbers of federal inspectors.

Question 9.: What is your response to criticism that the industry cannot be trusted to police itself?

This is totally at odds with the facts. In fact, railroads did not wait for the government to act before moving decisively to enhance security. Immediately after the events of 911, the industry mobilized a task force of outside security and terrorism experts to work with the industry to assess vulnerabilities and develop a comprehensive risk-based security plan. We were one of the first if not the very first industry to do that. The result was a comprehensive security plan that has been widely praised and resulted in more than 50 permanent changes in the way we do business. In addition, it outlines more than 100 additional actions railroads will take in response to credible threats at higher alert levels. Railroads did this because we take seriously the role we play in maintaining the safety and security of our employees, customers and the communities in which we operate.

Question 10. Doesn't the fact that since your members are in business to make money, there might be an incentive to cut corners on things like security from terrorist acts? Especially in light of the fact that the Administration doesn't seem to think rail security is a priority?

The exact opposite is true. It is because our members are in business to make money that there is an incentive to have as effective a security plan as possible. Any terrorist attack that disrupts the rail network would have a devastating impact on railroad service, revenues and profitability. Thus it is in our own self interest

not to cut comers on security—or safety for that matter—but rather to enhance it. Railroads do not cut corners when it comes to either safety or security, as evidenced by the fact that 2006 was the safest in history in terms of both train accident rates and employee casualty rates.

Question 11.: In 2007, 2 boys, a 16 and 13 year old, escaped from a juvenile detention home in Nelsonville, Ohio and took a 12 mile joyride in a stolen train before they were caught. **How can the American public have any peace of mind about the security of our nation's rail system when children can break in undeterred and commandeer a train?**

Terrorists can find far more accessible and vulnerable targets than can be reached through a stolen locomotive. The potential result of attempting to take a locomotive is far too uncertain for terrorists to find it attractive. They can find far more accessible and vulnerable targets elsewhere. The incident referred to in this question involved the Hocking Valley Scenic Railway, a short excursion railway that hauls tourists and operates largely with volunteers. Class I railroad employees receive robust safety and security training, and are trained to disable a train when it is unattended. It is doubtful those volunteers receive the same sort of security and safety training as do the employees of major freight railroads. Among other things, Class I railroad employees are trained to disable the locomotive when leaving it unattended.

Question 12.: What role, if any, did the federal government play in AAR's Terrorism Risk Analysis and Security Management Plan? Has DHS given you any feedback or guidance with regard to the plan? Have you shared this plan with the unions?

The Department of Transportation and the Department of Defense provided guidance to AAR in the conduct of risk analyses and the development of a 4-alert level security plan of action. For example, DOT'S Office of Security and Intelligence (S–60) and DOD provided threat information and assisted railroad staff in obtaining security clearances. AAR regularly consulted the Federal Railroad Administration throughout the planning process to ensure consistency with safety regulations. It should be remembered that DHS did not exist in 2001 when the railroads developed their security plan. FRA provided very positive feedback with respect to the industry plan. AAR has conducted several in-depth briefings for TSA officials and staff, including at least two briefings on risk assessment methodologies used by the industry. TSA has visited each of the Class 1railroads at least once to review how each railroad has implemented the industry plan. No corrective action has been required. AAR interprets this in a positive light even though TSA has not provided formal feedback on the industry plan to AAR.

To protect against divulging vulnerabilities, the detailed security plan is not available to labor unions, posted on web sites, or otherwise publicly available. A general description of the security plan has been available on our website for many years. Railroad employees, such as railroad police, operations officers, and IT security officers, who are responsible for carrying out specific actions at various alert levels are fully aware of their responsibilities and are periodically tested through industry table top exercises. Rank and file employees receive general security awareness training and, when the alert level changes, specific instructions in their areas of operation.

Question 13.: I was disturbed to read the article by Carl Prine, "Terror on the Tracks." **How can you explain a journalist being able to walk on a rail yard unchallenged and get close enough to hazmat shipments and other rail infrastructure to leave his business card behind? What was the response of your industry to this expose? What have you done to make our nation's rail yards more secure in light of this report?**

First and foremost we continuously remind our employees to report any suspicious activities or any suspicious individuals on railroad property. Securing the nation's rail network would be impossible if it depended upon always keeping people away from trains and tracks. The rail network includes 140,000 route miles, more than 1.3 million freight cars (including some 250,000 tank cars). To provide continuous and complete security along that entire network at all times is as impossible as it is to provide complete security along our nation's entire highway network and to every single tank truck. Mr. Prine could also have approached the millions of trucks in rest stops and placed his business card there, as well as on buses and passenger trains. But that would prove as little about the state of security for those modes as it does for rail security. The best security plan is one that is able to find out about an attack before it happens so that it can be prevented from happening at all. That is why railroads have adopted a plan that relies heavily on intelligence

to prevent an attack or take appropriate counter measures. It should also be noted that at this point, there has never been a credible threat of an attack on a U.S. freight train. Indeed, all terrorist attacks up to now have been on passenger trains, not freight trains.

Question 14.: TSA started working to secure the aviation system in late 2001; it was heavily criticized for not involving aviation stakeholders in its efforts. In response TSA committed to taking steps to enhance its coordination with stakeholders in the future. Is it your opinion that rail and mass transit stakeholders are appropriately involved as TSA moves forward with current and future security efforts, such as the recently issued proposed rule on rail?

AAR and individual railroads formally commented on the TSA notice of proposed rulemalung. It is vitally important for TSA to enhance coordination with the rail industry to avoid unintended negative consequences of government action. AAR and its member railroads are always available for TSA to consult, either through formal rulemaking or through the Critical Infrastructure Protection Advisory Council (CIPAC) process if security-sensitive matters are to be discussed. In addition, the AAR maintains a security Operations Center at the SECRET level should TSA wish to communicate classified threat information via secure communications.

Question 15.: TSA issued rail security directives in May 2004. **What was the industry's reaction to these standards and how could they be improved?**

The Association of American Railroads joined with then DHS Secretary Tom Ridge in a press conference to support the initiative. The directives were issued on an emergency basis following the Madrid bombings and apply to passenger rail operations and the freight railroads that host such operations. Now, three years later, TSA and all stakeholders should review the directives for their cost and effectiveness. Money devoted to implementing some of these directives might be better spent investing in more visible security measures, such as canine teams. Also, the role of TSA's surface transportation inspectors should be reviewed with an eye toward transforming them into operational security forces to add positive protection to rail passengers as federal air marshals provide to airline passengers.

Question 16.: TSA continues to emphasize the importance of carriers identifying and reporting security risks to homeland security officials. **Has your industry promoted whistleblower protections so that employees can report security concerns without fear of retaliation or retribution from employers?**

The safety and security of the nation's rail system is the industry's highest priority. Railroads strongly encourage their front-line employees, who are the industry's eyes and ears, to report any suspicious activity or behavior to their supervisor. Railroads do *not* object to equitable whistleblower protections for workers, but they do not believe that there should be one set of rules for whistle blowing on safety matters and a different set of rules for whistle blowing on security matters. Creating a new, separate system under the aegis of the Department of Labor is both unnecessary and potentially confusing.

Question 17.: TSA has recently issued a Notice of Proposed Rulemaking (NPRM) that would impose several new security requirements for rail carriers, rail transit systems, and rail operations at certain facilities that ship or receive hazardous materials. As part of this proposal, TSA would require rail and transit operators (as well as hazmat facilities) to allow physical inspection of their operations. In addition, chain of custody and hazmat tracking requirements will need to be enforced. **How many additional TSA inspectors do you anticipate will be needed for this expanded role? Do you agree with the rule?**

The Association of American Railroads does not take a position on the number of TSA inspectors that would be required to implement the NPRM. The nation's freight railroads have every incentive to secure hazmat shipments. If properly trained, TSA inspectors could provide operational security for hazmat shipments. The Association of American Railroads filed detailed comments on the TSA NPRM which are attached.

Question 18.: What effect will this rule have on your industry as a result of real world implementation?

The real-world impact depends upon the final rule. AAR explained in its comments that certain rule interpretations by TSA would create unmanageable situations for freight railroads, causing for example the shift of TM shipments off the rails and onto the highways.

Question 19.: Will this rule improve security of hazmat transport?

If properly structured, the rule could lead to enhanced security for hazmat shipments by rail.

Question 20.: It is my understanding that as drafted the NPRMs recently released by TSA and DOT will preclude state and local officials from mandating the rerouting of hazardous material. This seems very favorable to industry and detrimental to security of our high population urban areas. How can you justify this provision in the NPRMs?

It is important to recognize that federal preemption has been and remains an essential aspect of federal railroad safety law. The guiding principle underlying federal railroad safety law is that safety and efficiency are best promoted if one set of uniform regulations applies to railroads: preemption assures, consistent with the commerce clause, that different or conflicting requirements can't be imposed at the state or local level and that federal regulations must remain the standard of conduct for railroads nationwide;

In 1970, after extensive consideration, Congress concluded that because of the railroad industry's interstate nature, safety is best served by uniform nationwide regulations and that railroad safety would not be "advanced sufficiently by subjecting the national rail system to a variety of enforcement in 50 different judicial and administrative systems." Therefore, Congress gave the Secretary plenary power over rail safety and expressly preempted state law wherever the Secretary of Transportation has issued a regulation or order covering the subject matter of the state law. Since 1970, DOT has issued numerous regulations and orders governing many aspects of rail safety, regulations that are reviewed and updated as dictated by experience and new technology.

Without federal preemption, the railroads would be subject to innumerable state and local laws and ordnances. The result would be the disintegration of the efficient national rail network for hazardous materials transportation.

Mandatory rerouting would not eliminate risks, but would simply shift them from one place to another and from one population to another. In doing so, it could foreclose routes that are optimal in terms of overall safety and security. Because railroads have limited routing options, rerouting could add hundreds of miles and several days to a hazmat shipment. Additional switching and handling of cars could be needed, as could addtional dwell time in yards.

The result of these and other factors would likely be an increase in exposure to hazmat release and *reduced* safety and security.

Moreover, if hazmat transport were banned in one jurisdiction, other jurisdictions (including perceived "low threat7' areas that did not want to see increased hazmat traffic because of mandatory rerouting elsewhere) would be sure to follow suit. Already, numerous cities across the country are considering hazmat bans.

Banning hazmat transport by rail in even one city would be problematic, but banning them in cities throughout the country would virtually shut down hazmat shipments by rail. Indeed, the clarity and efficiency that uniform national standards bring would be lost if local andlor state governments could dictate what types of freight could pass through their jurisdictions. This problem would be especially acute for railroads, whose network characteristics and limited routing options mean that disruptions in one area could have profound impacts hundreds or thousands of miles away. These disruptions would negatively impact all rail traffic, not just hazmat traffic. For all these reasons, the provision of the NPRM maintaining federal preemption is appropriate.

An integrated, effective national network requires uniform standards that apply nationwide. If policymakers determine that hazmat movements should be banned, they should be banned nationwide, not locality-by-locality.

Question 21.: What do you feel is the carriers' role in providing security training for its employees?

Railroads provide general security awareness training for rank and file employees, including a training program developed by Rutgers University's National Transit Institute. Employees with specific responsibilities to carry out provisions of company security plans receive detailed instructions as to required actions at various threat levels and are tested periodically through industry table top exercises.

Question 22.: Do you wish you had more guidance from DHS on this issue?

Railroads are always open to new training materials and techniques. TSA has indicated it is developing employee security training with respect to EDidentification. Unfortunately, TSA has not coordinated this effort with the railroad industry. AAR is concerned that this training could cause an employee to put him or herself in harm's way which is contrary to industry policy.

Question 23.: Do you think TSA should mandate security training for mass transit employees?

The Association of American Railroads does not represent mass transit rail. This question should be posed to the American Public Transportation Association.

Question 24.: What are the costs of securing our rail and mass transit systems?

The Association of American Railroads does not represent mass transit rail and therefore cannot answer the question as it relates to mass transit systems. This question should be posed to the American Public Transportation Association.

With respect to the cost of securing the nation's freight rail systems, the AAR has not undertaken a comprehensive assessment of all security-related expenditures made by our member railroads since the implementation of the AAR's Terrorism Risk Analysis and Security Management Plan in 2001. This would be a difficult exercise as railroads' accounting systems do not contain a separate account for security expenses.

The Terrorism Risk Analysis and Security Management Plan which governs the security operations of the AAR's member railroads are risk-based. Costs associated with security measures are ramped up significantly as threat-level alerts are elevated. At the highest alert levels, the AAR estimates that railroads would not be able adequately to guard all critical infrastructure assets for an extended period of time. It is for this reason that the AAR seeks the cooperation of the state governors to deploy National Guard assets when such conditions would warrant.

The following provides a few examples of security expenditures by freight railroads:

- Railroad police programs (industry-wide, includes personnel, equipment, canines) $202 million annually, over $1 billion since 9/11). The entire amount arguably is not devoted to counter-terrorism per se, but at the same time it is often difficult to differentiate between counter-terrorism and police activity that provides security to railroad employees and the property of rail customers. Railroads carry large volumes of high-value commodities, the theft and sale of which could generate funds for terrorist activities;
- One railroad's redundant control center for disaster recovery ($15 million):
- One railroad's IT security, including system upgrades, labor and training ($15 million);
- DHS/CBP security requirements for cross-border rail transportation caused railroads to increase physical security and add technology such as CCTV, access controls and alarms. To accommodate CBP personnel who operate VACIS machines, railroads had to build new tracks and inspection facilities at border crossings. At one border crossing point, one railroad spent approximately $10 million for initial construction and overall security costs. The same railroad estimates expenses of $1.4 million for camera and sensor upgrades in 2007 and recurrent annual costs of adding resources at more that $300,00 at the same border crossing.
- Associated expenses due to train delays caused by CBP inspections have cost one railroad at least $1 million at that one border crossing.

Question 25.: How would you compare the risks facing the passenger rail systems with the risks faced by other modes of transportation? Is the current allocation of federal resources for rail security commensurate with the unique risks these systems face?

Based on an AAR and ST/PT–ISAC analysis of available threat information, the commuter and passenger rail systems face substantially greater risk of terrorist attack than the freight rail industry. While many terrorist attacks globally that have been directed at railroads transporting freight. AAR has no information regarding threats to other modes of transportation.

Question 26.: In your written testimony, you state that only "four of the seven Class 1 railroads are participating in e-RailSafe. What companies have not yet implemented the program?

The e-RailSafe program was instituted in late 2005. Of the seven Class 1 railroads, CSX, Canadian Pacific (CP) and Kansas City Southern (KCS) have not yet implemented the program. All have contracts with e-/RailSafe and plan to implement the e-RailSafe program in the near future.

Question 27.: Do you think that there is a substantial nexus between the disqualifying offenses and the jobs performed? If so, what is it?

The e-RailSafe background check program is designed to preclude employees of contractors who have been convicted of core crimes of concern from gaining access to Class 1 railroad property. Core crimes of concern include felony crimes against

persons such as assault, rape and murder, property crimes such as theft, burglary and arson, societal crimes such as people smuggling, narcotics crimes and prostitution, and federal crimes such as train wrecking. Persons convicted of-felony crimes determined by the railroads to be core crimes of concern are deemed potential threats to the railroad workforce, its property, and for customer shipments. Even when a conviction is not directly related to the job to be performed, the conviction may be considered an indication that a necessary personal qualification -integrity, reliability, honesty -is missing. Courts have also ruled that employers can be held liable for the damaging actions of their employees, including the employees of contractors, if based on that person's previous actions, he or she should have been disqualified for the job.

Question 28.: In your written testimony, you state that police are examining the disqualifiers used by individual railroads under the e–RailSafe program. What is the purpose of the examination?

The railroad police of the Class 1railroads are regularly reviewing the implementation of the e-RailSafe program. Part of this ongoing review includes efforts to standardize elements of the background check process among all member railroads. On March 6,2007, the railroad police agreed to a common list of core crimes of concern as automatic disqualifiers.

Question 29.: You have stated that the disqualifiers in the e–RailSafe program should not necessarily be the same as disqualifiers under government-sponsored programs. Why should the disqualifiers be different when consistency in "rolling out9' a program like this is of premiere importance?

The purposes of federal government credentialing programs (such as the transportation worker identification card (TWIC) and the hazardous materials endorsement (HME)) and the e- RailSafe program are very different. In the case of the TWIC, the federal government determined that the credentialing is required "to prevent those who may pose a security threat from gaining unescorted access to secure areas of ports."[1] It is an access control measure aimed at protecting ports against terrorist activity. The TWIC disqualifiers are ostensibly aimed at weeding out potential terrorists. As a consequence TWIC disqualifiers include crimes such as espionage, sedition, and treason. Other dsqualifying criminal offenses are included presumably as possible indicators that a person would be susceptible to committing terrorist activities.

In the case of the e–RailSafe program, the credentialing is required to prevent harm to the railroad's workforce, property and customer shipments. It is an access control measure aimed at protecting persons and property against harm from a variety of persons, not just would-be terrorists. The TWIC disqualifiers, for example, do not include felony theft, the unlawful use of controlled substances in violation of federal drug and alcohol rules, or attempted train wrecking. In the railroad environment, persons with such felony convictions in their immediate past represent a potential threat to railroad workers and property.

Question 30.: You go on to cite TWIC permanently disqualified as an example. Are you of the opinion that workers who commit these crimes should be able to work for rail companies within seven years?

The TWIC final rule lists 12 permanent disqualifiers including (1) espionage; (2) sedition; (3) treason; (4) a federal crime of terrorism; (5) a crime involving a transportation security incident; (6) improper transportation of a hazardous material; (7) unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, or storage of explosive devices; (8) murder; (9) making certain threats; (10) violations of RICO; (11) attempts to commit crimes 1—4;and (12) conspiracy or attempt to commit crimes 5—10.

The e-RailSafe program does not include any "permanent" disqualifiers. In general, member railroads are concerned with felony crimes that have occurred within the last 7 years.

Question 31.: If someone is convicted of a felony in one jurisdiction, but they are now working in a jurisdiction where the crime they committed is merely a misdemeanor, how is that reconciled?

The e-RailSafe program flags individuals who have felony convictions in their past, regardless of the jurisdiction in which they occurred.

Question 32.: With the appeals process recently agreed upon by rail companies, who in the company will hear an impacted worker's appeal?

---

[1] Transportation Worker Identification Implementation in the Maritime Sector; Final Rule, January 25,2007.

The background check appeals board within each railroad includes at a minimum three individuals: one from the railroad police force, one from human resources, and one from the legal department.

Question 33.: Chris Kozub from the National Transit Institute (NTI) has testified before our Committee on training for mass transit employees. In his testimony, he stated that NTI and FTA's training had reached about 20% of the transit employee workforce which is approximated to be about 300,000. As of today that number has increased to slightly higher than 30%. While reaching 90,000 employees—many of whom are employed by the larger, security critical, metropolitan systems of the country—is a noteworthy accomplishment, NTI is still below the halfway point and has a lot of work still to do. **Do you feel that this 'is adequate to give workers the tools they need to respond to or prevent a disaster?**

The Association of American Railroads does not represent mass transit rail. This question should be posed to the American Public Transportation Association.

Question 34.: Do you feel that the federal government should be responsible for ensuring that all employees receive training?

The railroads have already entered into a voluntary agreement with TSA regularly to reinforce security awareness and operational security concepts to all employees at all levels of the organization. As detailed in our testimony, the freight railroad industry is providing security training to the railroad workforce through a cooperative program with the Rutgers University National Transit Institute (NTI). Our industry takes seriously the responsibility to provide appropriate security training to our workforce. We do not believe it is the responsibility of the federal government to oversee the training of the nation's private sector workforce.

Question 35.: Is the President's budget request reasonable to help secure the nation's rail and mass transit systems? Is the disproportionately low amount of TSA's budget ($41.4 million out of $6.4 billion) dedicated to rail and mass transit security an indication to your organization that it is not a priority of DHS?

The Association of American Railroads has not taken a position on the President's budget request.

Question 36.: What are your thoughts in the utilization of security practices used by other countries? With which practices were you most impressed? Which do you think could be effectively implemented in the US?

AAR is not aware of unique practices used by foreign countries to secure freight rail operations. The North American freight rail industry is the envy of freight rail operators worldwide for its efficiency, safety, and security. AAR routinely hosts visitors from foreign countries who seek to learn the keys to a sound, privately-owned freight railroad network.

HON. KIP HAWLEY RESPONSES TO QUESTIONS FROM HON. BENNIE G. THOMPSON

Question 1.: What proactive measures has the Administration taken to prevent terrorist attacks to mass transit and rail infrastructure?

Response: The Department of Homeland Security (DHS) has consistently stated that mass transit security and passenger rail security are a shared responsibility among a variety of stakeholders, including state, local, and Federal agencies, and private owners and operators. The primary focus for the Department and the Transportation Security Administration (TSA) has been on information sharing, preparedness, domain awareness, training, and using a risk-based management approach to maximize the impact of available resources through random, visible security activities. We have employed wide-ranging strategies that engage our stakeholders and help ensure the security of mass transit and passenger rail systems. These strategies include:

- Regional Groups
- TSA Field Presence
- National Explosives Detection Canine Team Program
- Security Training
- Grant Programs
- Visible Intermodal Prevention and Protection Teams (VIPR)

Regional Groups

The creation of regional groups enhances coordination and improves communication among Federal, State, and local governmental partners and area mass transit stakeholders. This strategy has been implemented through various programs and initiatives in the past year. The creation of these groups helps to establish a forum

and process for more effective communication and information exchange among various governmental agencies and public transportation stakeholders. For example:

- Through the National Infrastructure Protection Plan (NIPP), the Department has established a forum and a process for more effective communication and information exchange among various agencies and with the public transportation stakeholders. In January 2006, TSA led the formation of the Transportation Sector Government Coordinating Council (TSGCC). Among its initial actions, the TSGCC called for the establishment of coordinating councils in each of the transportation modes.
- In March 2006, TSA led the effort to organize the Transit, Commuter and Long–Distance Rail Government Coordinating Council (TCLDR–GCC). This body brings together representatives from DHS, the Department of Transportation (DOT), TSA, the Federal Transit Administration (FTA), and the Federal Bureau of Investigation in a networked, collaborative process to develop consistent and effective security strategies and programs.
- The TCLDR–GCC engaged stakeholders in the passenger rail and mass transit communities to establish a Mass Transit Sector Coordinating Council. Participating entities include American Public Transportation Association (APTA), the Community Transport Association of America, and individual transit agencies representative of the community in system size and geographic spread.
- In support of these efforts, DHS established the Critical Infrastructure Partnership Advisory Committee (CIPAC) (as announced in the Federal Register on March 24, 2006 [Volume 71, Number 57, pages 14930–33]). CIPAC provides a process for engagement between GCCs and SCCs on a broad spectrum of collaborative security-related activities.
- In August 2005, the Department initiated the interagency Passenger Rail and Rail Transit Information Pilot Program. This program is aimed at knocking down any bureaucratic hurdles in the handling and dissemination of information by Federal entities. It ensures decision makers at all levels have a comprehensive and accurate picture of the state of passenger rail and rail transit security, and has streamlined procedures that improve communication and information sharing with stakeholders during both normal operating periods and emergencies. By integrating a network approach to the Federal Government entities involved in transit security, this program ensures the coordinating forums act upon timely and reliable information.
- TSA is working with DHS/G&T and DOT/FTA on developing the National Resource Center (NRC). The NRC will provide a comprehensive database allowing the transit industry to access information on a broad spectrum of subjects pertinent to transit security. Presently, this information is not readily available in any consolidated format. As an initial product of this effort, a periodic newsletter will be prepared and coordinated by TSA. This newsletter will provide items on Federal transit security initiatives; recent suspicious activity reporting with security context; and updates on model security practices observed in Surface Transportation Security Inspection program (STSI) assessments, technology programs, and other areas of interest. The newsletter will also incorporate effective security practices and items of general interest from transit agencies.

TSA Field Presence

Another key component of DHS's security strategy for rail and transit systems is TSA's field presence. We build upon the work done by the Department, the FTA, the Federal Railroad Administration, and industry, which has conducted numerous vulnerability and readiness self-assessments.

Through STSI, TSA has deployed 100 inspectors to 18 field offices across the country. These inspectors provide support to our Nation's largest railroads and mass transit systems, performing frequent inspections of key facilities, including stations and terminals, to identify potential threats. Inspectors are actively engaged in a range of security enhancement programs, such as assessing transit systems postures in implementing core transit security fundamentals and comprehensive security action items. Inspectors also conduct systematic examinations of stakeholder operations, including compliance with security requirements; identification of security gaps; and development of effective practices. The program's consistent presence and engagement with transit system security officials fosters an integrated approach to security enhancement efforts.

Field activities also assess compliance with security requirements and implementation of noncompulsory security standards and protective measures with the objective of a broad-based enhancement of passenger rail and rail transit security. Through the Baseline Assessment for Security Enhancement (BASE), inspectors re-

view the implementation by mass transit and passenger rail systems of the 17 Security and Emergency Management Action Items (security action items) that TSA and the FTA jointly developed, in coordination with the Mass Transit Sector Coordinating Council. This initiative aims to elevate security posture throughout the mass transit and passenger rail mode by implementation of baseline security measures adaptable to the operating circumstances of any system.

TSA's surface inspectors are actively engaged in performing Security Analysis and Action Programs (SAAPs), which constitutes a systematic vulnerability assessment of a mass transit or passenger rail system. The program utilizes several different tools to identify vulnerabilities based on specific scenarios, such as an IED on a passenger train. SAAPs can be conducted on individual critical infrastructure facilities or entire rail systems, with particular emphasis on critical control points. TSA focuses attention on six Transit Security Fundamentals that provide the essential foundation for a successful security program.

TSA deploys inspectors to serve as Federal liaisons to mass transit and passenger rail system operations centers and provide other security support and assistance in periods of heightened alert or in response to security incidents. TSA initiated this component of STSI program responsibilities in the aftermath of the attacks on the London transit system in July 2005. TSA inspectors are deployed to operations centers of transit systems in their areas to assess the security response and serve as liaisons for information and coordination of resource support from the Federal Government. Since this initial deployment, inspectors have developed relationships with security officials in transit systems in their areas, coordinated access to operations centers, participated in or observed exercises, and provided other assistance consistent with the overall objective of enhancing security through collaborative effort.

TSA conducts vulnerability assessments of High Threat Urban Area (HTUA) rail corridors where toxic inhalation hazard (TIH) shipments are transported. In December 2006, TSA introduced a package of new security measures that will require freight rail carriers to ensure 100 percent positive hand-off of TIH materials, establish security protocols for custody transfers of TIH rail cars in the high threat urban areas, and appoint a rail security coordinator to share information with the Federal Government, as well as formalizing TSA?s freight and passenger rail inspection authority.

Over the last year, detailed region-wide rail corridor assessments were completed in Houston, Buffalo, and northern New Jersey, and a fourth assessment is in the early stages of completion for the Los Angeles area. The HTUA corridor assessments provide site-specific mitigation strategies and lessons learned as well as tactics that can be modified for use at the corporate or national level. HTUA corridor assessments supported the development of the Recommended Security Action Items issued by DHS and DOT on June 23, 2006. These performance-based SAIs were developed to foster an enhanced security posture in the freight rail mode in general and specifically targeted the transport of TIH materials. These practices have been agreed to in binding commitments by the Nation's railways, and form the basis for pending regulation.

Buttressing these regional efforts is an expansion of explosives detection capabilities. The Department is aggressively testing screening technologies, with an emphasis on practical use in a transit environment and mobility. These new technologies include:

- Developing and deploying chemical detection equipment in segments of the Washington, D.C., New York City, and Boston rail systems;
- Testing the "movable checkpoint" equipment, which can fit into two standard-size shipping containers and be rapidly deployed for use in screening and detection at any major system in the country in a particular threat situation;
- Developing new surveillance camera systems designed to detect human anomalous behavior for use with surveillance/closed circuit television camera systems;
- Evaluating new explosives detection equipment by field testing its effectiveness in partnership with the Port Authority of New York and New Jersey; and
- Testing a detection system in Baltimore in partnership with the Maryland Transit and State authorities to ascertain its ability to identify explosive compounds on passengers before they board a train.

By continuing these initiatives, the Department plans to identify optimal technological solutions that expand detection capabilities for explosives and chemical, biological, and radiological weapons.

National Explosives Detection Canine Team Program

Through the National Explosives Detection Canine Team program, teams are being trained, certified, and deployed by TSA to passenger transit systems. Since

late 2005, TSA's National Explosives detection Canine Team Program has worked in partnership with passenger transit systems to train, certify, and deploy 53 explosives detection canine teams to 13 major systems in a risk-based application of resources. Forty of these teams are currently in place and 13 are projected for training, certification, and deployment in the coming months.

The TSA-trained and certified teams provide strong detection and deterrent capabilities and can be sent quickly to key junction points across systems, stations, terminals, and other facilities. This resource provides a visible and effective detection and deterrence presence in the public transportation system and can be surged to other venues as threats dictate. Teams can post at key junctions or points within systems, stations, terminals, and facilities, and deploy throughout rail systems. Random deployment heightens the deterrent effect. The Department provides funding, training, and management to the National Explosives Detection Canine Team program.

Security Training

Training and public awareness are crucial, strategic underpinnings to enhancing rail security. DHS is involved in several training initiatives, including:

- Funding several Land Transportation Anti–Terrorism Programs that provide training to local authorities in protecting land transportation infrastructure, including rail, light rail, and mass transit;
- Partnering with the FTA on Connecting Communities, a series of forums to help transportation and emergency response agencies work together to prepare and protect their communities;
- Working on the development of an interactive computer-based program for both passenger and freight rail employees to provide the knowledge and skills necessary to identify security threats, observe/report suspicious activities and objects, and initiate action to mitigate, or recover from, a threat or incident; and
- Supporting the Transit Watch Program, led by FTA, which provides a nationwide safety and security awareness program to passengers and employees through both printed materials and CD–ROM format.

Grant Programs

To foster continued development of effective transit security programs, the Department administers the Transit Security Grant Program (TSGP) focused on rail transit, intracity bus, and ferry systems. A network integrating the Department's Office of Grants and Training, TSA, and FTA has been established to provide assistance to eligible transit systems in completing applications for award. Both in funding allocations and priorities, this year's program reflects the Department's risk-based approach to security.

The program guidelines and application materials were recently published. Factors considered in evaluating proposals include the enhancement of capabilities to: (1) deter, detect, and respond to terrorist attacks employing improvised explosive devices; (2) mitigate high consequence risks identified in individual transit system risk assessments; (3) implement technology for detection of explosives and monitoring for suspicious activities; (4) improve coordination with law enforcement and emergency responders; and (5) expand security training and awareness among employees and passengers.

TSA uses the TSGP to drive improvement in the six security fundamental areas mentioned earlier, including training for key personnel, drills and exercises, and public awareness and preparedness. The $175 million TSGP is the centerpiece of DHS's interagency strategy to close gaps between operator security status and baseline standards. For purposes of the TSGP, "transit" includes Amtrak, which is eligible for $8.3 million, and commuter ferry systems, which are eligible for $7.8 million. The TSGP guidance emphasized the six fundamental principles as well as efforts in support of the national preparedness architecture. We expect to direct transit grant awards based on our system assessments, security fundamentals, and support of national preparedness. DHS leverages the grants program to close the gaps at high risk properties.

For example, in Mass Transit, attacks by improvised explosives devices (IEDs) presented high risk; our field assessments determined that lack of training was a vulnerability, and we applied grants funding to close the gap. Alread implemented and showing results. TSA considers this to be an effective strategic approach.

VIPR Teams

Additional security resources are applied through the development of VIPR Teams, which are deployed randomly. VIPR teams add to TSA's strategy of layered security, and introduce an element of unpredictability to disrupt potential terrorist planning activities. Consisting of personnel from the Federal Air Marshal Service

(FAMS), STSI, and explosives detection canine teams, VIPR teams were created as a way to prepare for emergency situations in which TSA assets would be invited to assist a local transit agency. VIPR teams allow TSA and local entities to develop templates that can be immediately implemented in emergency situations. FAMS participation in VIPR deployments are planned for brief periods and are scheduled not to interfere with normal aviation operations. Using advanced screening technology, these teams provide the capability to leverage a variety of resources quickly and effectively. The deployments are designed to raise the level of security anywhere in the country. The teams work with local security and law enforcement officials to supplement existing security resources and provide deterrent presence and detection capabilities. More than 25 VIPR exercises have been conducted at key commuter and regional passenger rail facilities, and more are planned throughout 2007.

Question 2.: Each mode of transportation presents its own risks. **How would you characterize the risks faced by passenger rail systems? How would you compare these with the risks faced by other modes of transportation? Is the current allocation of federal resources for rail security commensurate with the unique risks these systems face?**

Response: The Transportation Security Administration (TSA) takes a network approach to transportation security and views it as a shared responsibility and effort among all of TSA; the Department of Homeland Security (DHS); other government agencies and entities at all levels, including Federal, State, local, tribal and territorial; and owner-operators.

The difference in Federal funding for aviation and surface transportation does not present the complete picture. Whereas Federal funding constitutes a substantial portion of aviation security monies, the Federal portion for surface transportation security constitutes a much smaller percentage of the total spent for surface transportation. When the money spent by private industry, states, and localities is added to the Federal portion, the total funds for surface transportation security are commensurate with the risk.

Much of the Nation's aviation infrastructure is federally owned. Surface modes of transportation are approximately 95 percent privately owned and operated. They receive security funding support from multiple streams (i.e., State, local, private, as well as Federal). The Department has consistently stated that responsibility for surface transportation security is a shared responsibility among a variety of stakeholders, including State, local, and Federal agencies, and private owners and operators. The appropriate role for the Federal government includes: using the substantial resources already in place and providing critical information; setting national priorities; developing transportation security fundamentals; coordinating ongoing efforts; and encouraging certain actions that reduce risk to the Nation's transportation system.

The bulk of Federal spending in aviation security has covered the compensation and benefits of Transportation Security Officers, who work every day in more than 450 airports nationwide to ensure the skies remain secure. Aviation security allows for point defense. We can seal off an area of the airport and only permit entry to those with tickets who have passed through screening.

The rail and mass transit modes do not accommodate this type of approach. These systems operate over a broad geographic spread with numerous stations and transfer points providing the efficiency and fast-pace that are essential to moving thousands of passengers, particularly during daily rush hours. The point defense approach taken at the airports is neither practicable nor desirable. Rather, an integrated strategy, tapping the strengths of the Federal government, State and local governments, and passenger rail and mass transit agencies, must be pursued.

In evaluating the resources required to address surface transportation risk issues, it is important to take into account not just TSA's budget and statutory obligations in aviation, but also the substantial efforts, capabilities and expertise that already exist in the surface transportation environment, as well as very different operating, legal, and resource requirements. Therefore, the level of TSA's budget allocated to surface transportation security relative to aviation does not and cannot reflect the overall relative risk between them. In fact, TSA does give attention and priority to surface transportation, but TSA's role relative to the security partners in the networked approach is different than it is in aviation.

TSA has looked across all modes of transportation and set risk-based priorities. These priorities are used to focus TSA's attention and resources on the most critical issues. TSA has conducted or participated in various risk analyses that compare risks across different transportation modes, including most recently the DHS Strategic Homeland Infrastructure Risk Assessment (SHIRA). Surface transportation,

transit, and rail are currently high priorities for TSA. The level of funding is determined by the degree to which TSA can effectively mitigate the risks, compared to the degree with which industry and other stakeholders are able to mitigate the risks.

For transit, a top priority is high density passenger transit systems in urban areas with underwater or underground tunnels. The risk of an improvised explosive device attack in a mass transit environment has been repeatedly demonstrated throughout the world, including London, Madrid, and India. Consequently, TSA augmented its security efforts in Mass Transit to include: Visual Intermodal Protection and Response (VIPR) teams; bomb-sniffing dogs; assistance with training and managing system-owned explosive detecting canines; and a range of pilot and experimental screening, detection, and deterrence programs.

In addition, TSA is also working to improve the risk basis for the Transportation Security Grant program. While the criteria for allocating grants among large transit systems continue to evolve, the criteria for approving specific project plans for actually spending the money is tightly focused on projects that mitigate prioritized risks.

Question 3.: What methods are being used to analyze and characterize the nature of various risks to rail and other modes of surface transportation?

Response: The Transportation Security Administration (TSA) has been working continuously to update and expand its assessments of threats and vulnerabilities in the transportation sector. TSA uses these assessments in conjunction with our security partners in government and industry to mitigate risk by operationalizing intelligence and addressing vulnerabilities.

Headquarters Analysis

TSA's layered approach to security seeks to identify and deter threats well before they reach the Nation's airports, railways, highways, mass transit, ports and pipelines. Transportation-specific intelligence is critical to TSA's overall risk-based security strategy, and its products provide a threat framework to prioritize security resources and operationalize intelligence. Two of TSA's operational programs have field units—the Office of Security Operations, which is responsible for both aviation Transportation Security Officers (TSO) screening and surface inspector operations, and the Office of Law Enforcement, which is responsible for the Federal Air Marshal Service (FAMS). These elements incorporate intelligence into their operations and plans on a daily basis, acting or deploying on the basis of the latest information.

TSA also coordinates closely and shares information with other Department of Homeland Security (DHS) components, the intelligence and law enforcement communities, other government departments and agencies, such as the Department of Transportation (DOT), and the transportation industry. These security partners provide intelligence and, especially in industry, are often well-positioned to operationalize transportation-specific intelligence by adjusting their business or security operations.

TSA's Office of Intelligence has produced classified and unclassified annual threat assessments for each transportation mode and the cargo/supply chain sector since 2004. These reports are disseminated throughout TSA, DHS, and private industry. Other Office of Intelligence products include:

- Transportation Intelligence Gazette
- Special Threat Assessments
- Weekly Field Intelligence Report
- Suspicious Incidents Report
- Intelligence Notes
- Transportation Situational Awareness Notes

TSA is also conducting specific analyses related to underwater mass transit tunnels. In October 2006, an Underwater Tunnel Working Group was established consisting of members from various DHS and DOT entities. This interagency team has taken significant steps to identify vulnerabilities of underwater tunnels and implemented aggressive mitigation strategies to protect high-risk and high-consequence tunnel infrastructure in both the short and long term.

Field Assessments

At the field level, TSA conducts various assessments which are either explicitly vulnerability assessments or at least provide vulnerability-related information. In all cases, they further TSA's risk-based security strategy and are described below.

Corporate Security Reviews

A Corporate Security Review (CSR) evaluates corporate level security policies, practices, and procedures. Specific CSR evaluation criteria have been established for the pipeline, rail, and highway modes. The CSR criteria identify a desired baseline

of security for a company, and the accumulation of individual assessments establishes an actual baseline in a given industry or mode, as well as potentially identifying best practices and common concerns.

In the highway mode, TSA entered into agreements with 37 State departments of transportation or bridge administrations to conduct CSRs of their facilities and critical infrastructure. In addition, TSA conducts CSRs of motor coach, school bus, and trucking companies. By the end of fiscal year 2006, 71 CSRs had been conducted in the highway mode. Additionally, 950 CSRs were conducted by the Missouri Commercial Motor Vehicle Inspectors under a pilot project that TSA is currently evaluating.

In the pipeline mode, a total of 54 CSRs have been conducted, including seven reviews in fiscal year 2006 with companies that represent approximately 60 percent of the product transported through the Nation's pipelines. In addition, TSA has joined with Natural Resources Canada to conduct four security assessments for critical cross-border energy pipeline systems.

TSA has also developed a CSR program in the rail mode and will be conducting assessments in spring 2007.

TIH Rail Assessments

TSA conducts vulnerability assessments of High Threat Urban Area (HTUA) rail corridors where toxic inhalation hazard (TIH) shipments are transported. Over the last year, detailed region-wide rail corridor assessments were completed in Houston, Buffalo, and northern New Jersey, and a fourth assessment is in the early stages of completion for the Los Angeles area. The HTUA corridor assessments provide site-specific mitigation strategies and lessons learned as well as tactics that can be modified for use at the corporate or national level. HTUA corridor assessments supported the development of the Recommended Security Action Items (SAI) issued by DHS and DOT on June 23, 2006. These performance-based SAIs were developed to foster an enhanced security posture in the freight rail mode in general and specifically targeted the transport of TIH materials. These practices have been agreed to in binding commitments by the Nation's railways, and form the basis for pending regulation.

Surface Transportation Security Inspectors (STSI)

BASE Reviews

Within the last year, the STSI program has conducted 26 Baseline Assessments for Security Enhancement (BASE reviews) as part of a program to conduct security reviews of the 50 largest transit systems nationwide. The BASE process reviews security procedures put in place by a transit (rail and bus) system to assist in evaluating the performance of its security system. BASE is not a compliance inspection, but rather a collaborative effort between the stakeholder and TSA. No enforcement actions occur as a result of BASE. To conduct this joint review, STSIs meet with security representatives of the transit agency to review the agency's pertinent documents.

Security Action Items (SAI))—Non-regulatory inspections

To gain an understanding of the degree of implementation across the Nation, railroad carriers of TIH materials, DHS and DOT agreed to conduct SAI Implementation Surveys (SAIIS) of freight rail operations. These surveys are conducted by STSIs. The surveys are not compliance inspections, but rather assessments to determine the depth and degree of employee security awareness and security action item implementation. The results of the SAI Surveys will be reviewed and the data used to guide future policy decisions regarding the security of hazardous material rail shipments. Since October 2006, STSIs have conducted 165 field site visits of freight railroad yards and facilities and interviewed 2,600 front line railroad workers.

Security Analysis and Action Programs (SAAP)—Risk Assessments

STSIs conduct Security Analysis and recommend an Action Program. SAAPs are full risk assessments of transit and rail systems. They are not compliance inspections. An SAAP assessment rigorously analyzes the likelihood and consequence of the threat stream matrix for the rail environment and analyzes the effectiveness of countermeasures to manage risk effectively. SAAPs leverage the DHS Vulnerability Identification Self Assessment Tool (VISAT).

The STSI program has completed full SAAP assessments on the following rail systems:

- Virginia Railway Express
- Alaska Railroad
- Tri—Met (Portland, Oregon)

Question 4.: TSA has recently issued a Notice of Proposed Rulemaking (NPRM) that would impose several new security requirements for rail carriers, rail transit systems; and rail operations at certain facilities that ship or receive hazardous materials. As part of this proposal, TSA would require rail and transit operators (as well as hazmat facilities) to allow physical inspection of their operations. In addition, chain of custody and hazmat tracking requirements will need to be enforced. **How many additional inspectors does TSA anticipate will be needed for this expanded role? Will additional funds be necessary?**

Response: Initial rollout of the Transportation Security Administration's (TSA) rail transportation security final rule will be handled with existing resources. TSA is currently evaluating any additional requirements. We anticipate that the Surface Transportation Security Inspectors (STSI) will inspect railroads and rail chemical facilities for adequate physical security measures surrounding rail secure areas and records documenting a proper chain of custody, completion of the Department of Transportation's requirement for a security inspection, and the appointment of a Rail Security Coordinator.

Question 5.: How would you characterize TSA's efforts in securing the passenger and freight rail system? What should be the federal government's top priority in securing the passenger rail system?

Response: The Transportation Security Administration (TSA) pursues a risk-based, threat managed, layered approach to security in transportation, including passenger rail, mass transit, and freight rail. This approach starts by leveraging the work of other U.S. Government and allied foreign entities through effective gathering, analysis, and dissemination of intelligence and through information sharing.

The disruption of the terror plot in the United Kingdom in summer 2006 and other threats illustrate the necessity of this approach. The best defense is one that prevents the terrorists from ever entering the United States. Aviation system security measures provide a significant barrier to entry for potential terrorists coming to our country. Our government's investments and improvements in terrorism watch lists, border security, and intelligence networks significantly enhance surface transportation security. As a strategic and operational priority, TSA complements these efforts by pursuing the expansion of visible, unpredictable deterrence environments in our surface transportation systems to disrupt terrorists? planning and preparation activities and execution of their missions.

In securing transportation systems, we employ a network approach. While each transportation mode has its own security challenges, there are common vulnerabilities and mitigation strategies. In an effort to employ the range of security resources most effectively, we work closely with transportation networks to leverage our security impact and determine risk-based priorities.

Building on this approach, TSA implements a comprehensive strategy that applies a common methodology across all transportation networks, regardless of mode. That strategy is straightforward. It consists of five elements:

- Assess industry threat, vulnerability, and consequence;
- Develop baseline security standards;
- Assess actual security status against baseline security standards;
- Develop plans to close gaps between actual status and baseline security standards; and
- Develop enhanced systems of security.

The top priorities in passenger rail security are encompassed within three guiding principles for the application of these elements:

- Focused effort to mitigate high consequence risk;
- Expanded employment of random, unpredictable deterrence; and
- Elevation of the security baseline through training, drills and exercises, and public awareness campaigns.

Question 6.: As TSA started working to secure the aviation system in late 2001, it was heavily criticized for not involving aviation stakeholders in its efforts. In response, TSA committed to taking steps to enhance its coordination with stakeholders in the future.

What steps is TSA taking to ensure that rail and mass transit stakeholders are appropriately involved as it moves forward with current and future security efforts, such as the recently issued proposed rule on rail?

Response: A close partnership and information sharing with stakeholders is paramount to enhancing the security of mass transit and passenger rail and is an integral element of the Transportation Security Administration's (TSA) overall strategy. We are furthering this strategy through constructive engagement with governmental security partners; communications with transit system operating and secu-

rity officials; regional collaboration, and semiannual roundtables with transit officials.

TSA operates in the framework developed under the National Infrastructure Protection Plan to ensure effective engagement and coordination with rail and mass transit stakeholders. On the Federal side, the entities responsible for rail and transit security have organized in Government Coordinating Councils (GCCs); these are, respectively, the Freight Rail GCC and Transit, Commuter and Long Distance Rail (TCLDR) GCC. Stakeholders in these modes have organized into Sector Coordinating Councils (SCCs), respectively the Freight Rail SCC and the Mass Transit SCC, bringing together key management and trade association officials in these industries.

The councils meet independently to develop priorities and positions and jointly to develop and implement security strategies and programs. The Critical Infrastructure Partnership Advisory Council (CIPAC), established by Secretary Chertoff to cover all critical infrastructure sectors, provides the process that enables consensus-based engagement among the councils. Intermodal issues are addressed by the Transportation Sector GCC under this process.

TSA has utilized the Freight Rail Sector Coordinating Council (FRSCC) as a means to include stakeholders in developing programs and policies to enhance the security of the freight rail network. The FRSCC was one mechanism in the development of the Freight Rail Modal Implementation Plan, an annex to the Transportation Sector Specific Plan. Additionally, TSA has developed and continually refines stakeholder relationships through the High Threat Urban Area Rail Corridor Assessments. In this capacity, stakeholders, including the affected carriers, and State and local government entities are involved in assessing high traffic rail corridors to identify mitigation strategies.

In the passenger rail and mass transit mode, TSA has established the Transit Policing and Security Peer Advisory Group. Formed under the auspices of the GCC/SCC framework, TSA works with transit agency security professionals to harness the application of resources and the development of programs to maximize the impact in enhancing security. The Advisory Group brings together the expertise of 13 transit police chiefs and security directors from systems across the Nation as a sounding board and liaison group to advance effective security programs.

To advance regional engagement and maximize application of available security resources, TSA is leading the formation of regional public transportation GCCs and encouraging public transportation stakeholders in metropolitan areas throughout the United States to form regional SCCs. These councils will foster development and communication of coordinated policies and positions on matters in transportation security and operational efficiency. Members of the respective councils will engage in collaborative efforts to develop and implement security strategies, plans, and programs under the CIPAC. Through regional engagement and regional deployment of resources, TSA seeks to advance the use of a full spectrum of available resources from Federal, State, and local governmental entities and the area transit systems in a concerted effort to disrupt the terrorists' ability to orient planning and preparation activities. This regional deployment approach entails developing and implementing a sustainable program to elevate security posture through information sharing, visible and random deterrent activities, and enhancing vigilance through security training and awareness programs.

Twice yearly, TSA and the Federal Transit Administration host Transit Security Roundtables, bringing together the security chiefs and directors of the Top 50 transit agencies (by passenger volume) in a working group forum to tackle specific security challenges.

Question 7.: Why hasn't TSA required security training for rail and mass transit employees?

Response: The Federal Government currently has security training requirements in place in both passenger and freight rail. The Transportation Security Administration and the Federal Transit Administration's (FTA) Rail Fixed Guideway Systems: State Safety Oversight Rule, title 49, Code of Federal Regulations (49 CFR), section 659.19 (k)(7), requires that system safety plans include the process used by the rail transit agencies to develop an approved, coordinated schedule for employee emergency training activities.

With regard to passenger rail, the Federal Railroad Administration (FRA) regulation on passenger train emergency preparedness,I CFR Part 239, applicable to certain commuter or other short-haul passenger train service and intercity passenger train service, requires employee training as a component of the required emergency preparedness plan. The regulation states that the plan shall address individual employee responsibilities and provide for initial training, as well as periodic training

at least once every two calendar years thereafter, on the applicable plan provisions. At a minimum, the initial and periodic training must include:

(A) Rail equipment familiarization;
(B) Situational awareness;
(C) Passenger evacuation;
(D) Coordination of functions; and
(E) Hands-on instruction for location, function, and operation of on-board emergency equipment.

The requirement also applies to control center personnel and requires that they be provided with initial training, as well as periodic training at least once every two calendar years thereafter, on appropriate courses of action for each potential emergency situation. At a minimum, the initial and periodic training must include:

(A) Dispatch territory familiarization and
(B) Protocols governing internal communications between appropriate control center personnel when an imminent potential emergency situation exists.

Moreover, with regard to freight rail, the Department of Transportation (DOT) currently requires security training for all hazardous materials employees in freight rail transportation (49 CFR 172.704).

Additionally, TSA works collaboratively with rail and mass transit stakeholders to enhance the scope and quality of security training. This approach encompasses multiple components:

- Coordinating with rail and mass transit stakeholders through the Mass Transit Sector Coordinating Council and Freight Rail Sector Coordinating Council to identify and address difficulties and deficiencies in training efforts;
- Issuing of Security Action Items for the rail and mass transit modes with security training for employees as a key element;
- On-site assessment of security posture in the Security Action Items by TSA Surface Transportation Security Inspectors;
- Setting targeted counterterrorism training for front-line employees—one of the six Transit Security Fundamentals that are the foundation of an effective security program—as a strategic priority and funding priority under the Transit Security Grant Program (TSGP); and
- Implementing an expedited training initiative under the TSGP that assists transit agencies in the difficult task of freeing employees for training programs through targeted funding.

The Mass Transit Security Training Program identifies specific types of training at basic and follow-on levels for particular categories of transit employees. Presented in a readily understandable matrix, it provides effective guidance to transit agency officials in building and implementing training programs for employees working in their systems. To support execution of such training programs, the TSGP offers pre-packaged training options agencies may obtain with grant funding. Agencies taking advantage of this program have their applications expedited for approval to ensure funds are delivered within 90 days of submission. This initiative aims to expand significantly the volume and quality of training for transit employees during 2007. Thus far, 21 agencies have applied for training under this initiative among the Tier 2 systems alone for fiscal year (FY) 2007 TSGP funding. Nine other transit agencies proposed training in their standard fiscal year 2007 TSGP applications.

Question 8.: Is there yet a list, consolidated by TSA on the security courses available to front line rail and mass transit employees?
If not, why not?

Response: Yes. The Transportation Security Administration (TSA), in coordination with the DHS Office of Grants & Training and the Federal Transit Administration, developed the Mass Transit Security Training Program, which identifies specific types of training at basic and follow-on levels for particular categories of transit employees. Presented in a readily understandable matrix, the Program provides guidance to transit agency officials in building and implementing training programs for employees working in their systems. To support execution of such training programs, the TSGP offers pre-packaged training options agencies may obtain with grant funding. Agencies taking advantage of this program have their applications expedited for approval to ensure funds are delivered within 90 days of submission.

In freight rail, TSA has reviewed existing training materials produced by the Association of American Railroads. Each railroad may have training materials to supplement these courses. TSA reviews corporate training materials through its Corporate Security Review program. After completing a Corporate Security Review, TSA has a comprehensive understanding of the training courses available to a company's employees and can work with them on an necessary improvements.

Congress created TSA as the one agency responsible for transportation security. Why won't TSA take the lead on these issues?

Response: The Aviation and Transportation Security Act established the Transportation Security Administration (TSA) as the lead in transportation security for mass transit and rail. Additionally, Congress has given responsibility and funding for safety and security activities to the Department of Transportation (DOT). With TSA as the lead, the Department of Homeland Security, in cooperation with DOT and other federal agencies, and in partnership with public and private sector owners and operators, has taken significant steps to enhance mass transit and rail security. For example, the development and distribution of the Mass Transit Security Training Program, supported by the expedited training application initiative under the Transit Security Grant Program (TSGP), demonstrates TSA leadership in this vital area. TSA initiated this effort in direct response to the results of the ongoing dual-track security assessment initiative.

Under the Baseline Assessment for Security Enhancement (BASE) program, TSA Surface Transportation Security Inspectors (STSIs) assess transit agencies? posture in 17 Security and Emergency Management Action Items encompassing a range of areas essential to an effective security program such as:

- Security and emergency management planning;
- Risk and vulnerability assessments;
- Implementation of random, unpredictable deterrence;
- Training, drills and exercises;
- Public awareness campaigns; and
- Facility, personnel, and information security.

A concurrent initiative involves transit agencies conducting self-assessments on six fundamental areas and reporting the results to TSA.

The assessment results demonstrated the need for more focused effort in security training for transit agency employees. Although an extensive Federal security training program has been implemented since 9/11—17 security courses, more than 500 deliveries, and more than 90,000 transit employees trained—the assessment results indicated wide variations in the quality of transit agencies' security training programs and an inadequate level of refresher or follow-on training. Well-trained employees are a security force multiplier for security efforts implemented by transit agencies. To elevate the level of training generally, bring greater consistency, and assist agencies in developing and implementing training programs, TSA produced and disseminated the Mass Transit Security Training Program.

TSA will continue to apply assessment results to drive strategic priorities, security programs, and allocation of resources.

If so, has this information been disseminated to the stakeholders and relevant agencies?

Response: Yes, stakeholders and agencies have been informed through Information Bulletin 243 (IB–243), issued under the Transit Security Grant Program (TSGP). The information has also been provided directly to the Mass Transit Sector Coordinating Council (SCC) and the Transit Security and Policing Peer Advisory Group. Finally, the Transportation Security Administration (TSA) has posted the information on the Public Transit Portal of the Homeland Security Information Network.

Question 9.: TSA failed to include any training requirements for front-line rail workers in the recently released Notice of Proposed Rulemaking concerning the movement of hazardous material by freight rail. **Can you explain to the Committee why TSA again missed an opportunity to impose a training requirement for these workers?**

Response: The Department of Transportation (DOT) currently requires security awareness training for all hazmat employees. DOT's Pipeline and Hazardous Materials Administration currently requires security training of all hazardous materials (hazmat) employees in freight rail transportation (49 CFR 172.704). Title 49 CFR 171.8 defines a hazmat employee as a person who in the course of their employment directly affects transportation safety. The term hazmat employee specifically covers persons who "load, unload, or handle hazardous materials," "[prepare] hazardous materials for transportation," "are responsible for the safety of transporting hazardous materials," or "[operate] a vehicle used to transport hazardous materials."

Employers must provide hazmat employee training, which includes the following:

- General awareness/familiarization training;
- Function-specific training;
- Security awareness training, which must include a component covering how to recognize and respond to possible security threats;

- In-depth security training, which must include information concerning the company security plan and its implementation, company security objectives, specific security procedures, employee responsibilities, actions to take in the event of a security breach, and the organizational security structure; and
- Recurrent training every three years.

To supplement this requirement, the Department of Homeland Security (DHS) and DOT issued Security Action Items (June 23, 2006) that recommend that toxic inhalation hazard rail carriers "regularly reinforce security awareness and operational security concepts to all employees at all levels of the organization."

TSA Surface Transportation Security Inspectors are currently assessing the level of security awareness training throughout industry to identify gaps in employee security knowledge. After reviewing training videos produced by the railroad industry, we determined that videos are a good starting point, but additional training materials are necessary. TSA is in the final stages of producing an improvised explosive device Recognition Training Video for railroad employees. Further DVD video training programs are planned including identifying and reporting suspicious activity and behavior.

Question 10.: What steps has the Department taken to develop a robust research and development program for rail and mass transit security? I know that there have been a few initiatives in the past like TRIP and the pilot in Maryland last year, but these initiatives appear to me to be piecemeal.

Response: The Transportation Security Administration (TSA) participates in the Integrated Process Teams (IPT) convened by the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) across a variety of critical infrastructure and potential threats. These IPTs provide a means to submit technology requirements for funding and coordinate requirements with other DHS internal stakeholders (i.e. Customs and Border Protection, United States Coast Guard) to eliminate duplication of effort and share experience and knowledge. The coordinated effort has harnessed research and development resources effectively to advance TSA's strategic priorities. These include protection of underwater and underground infrastructure (transit tunnels are a top priority for research and development of hardening and security enhancement technologies) and development of mobile and fixed systems amenable to the demands of the transit environment that may be deployed flexibly for maximum deterrent effect and protection of high risk infrastructure. Pilot testing will employ equipment in this manner to validate capabilities most effectively and deliver deterrent effects. Future research and development initiatives will maintain this focus.

Question 11.: To date, how much has the Department spent on research and development for rail and mass transit?

Response: In fiscal year 2006 DHS S&T executed $7M towards a Rail Security Pilot (RSP) charged with demonstrating explosive screening technologies, concepts of operations, and training to reduce the threat of suicide and leave-behind bombers in the heavy rail (e.g., subway) mass transit environment. The pilot was broken into two phases; phase 1 consisted of off-the-shelf technologies while phase 2 demonstrated prototype technologies. These pilots were conducted at the Port–Authority Trans–Hudson's (PATH) Exchange Place Station in Jersey City, NJ; the Baltimore Metropolitan Transit Authority's Johns Hopkins station in Baltimore, MD; and the Atlanta MARTA Five Points and airport stations.

The RSP performed market studies to identify potential candidate technologies for field testing, conducted lab tests to qualify potential technologies for field testing, worked with host authorities to develop viable concepts of operations, instrumented the test site to collect key data necessary for model benchmarking and to assess the pilot's effectiveness, installed the equipment at the host site, conducted pilot operations and conducted operations experiments, and provided feedback to the equipment vendors on their systems to accelerate the development of screening equipment for the rail environment.

Millions of dollars have been spent on developing technologies associated with protecting people and infrastructure in the transportation sector above and beyond the RSP. Some of the projects that have a direct application to protect rail and mass transit are listed here.

- BioWatch
- PROTECT chemical detection system
- Motivation and Intent—Project Hostile Intent
- Automated Scene Understanding
- Improvised Explosive Device and Leave-behind Bomb Detection
- Cargo Security

- Autonomous Rapid Facility Chemical Agent Monitor
- Lightweight Autonomous Chemical Identification System
- Low Vapor Pressure Chemical Detection Systems
- Explosives Detection Research
- Explosives response capabilities including Bomb Assessment tools and Render Safe technologies
- Explosives Conveyance Protection

In addition, the Office of Infrastructure Protection (IP) has developed the National Capitol Region Rail Pilot Project (NCRRPP). The NCRRPP is an intelligent video-based security program that provides security enhancements along an 8.1 mile rail corridor that runs through Washington, D.C., that is owned and/or operated by CSXT and Amtrak. The CSXT concept for this security pilot project was developed following the Madrid rail bombings in March 2004 and was later expanded to include an Amtrak portion as a result of the London Bombings. The CSXT portion runs from the Long Bridge to the Benning Rail Yard and includes critical areas such as 14th St. (Long Bridge), L?Enfant Plaza and the Virginia Avenue Tunnel. The Amtrak portion includes the virtual fence system described in other sections of this response and also substantial work in the buffer zone area around Union Station, the cargo area and places where unauthorized personnel can enter the tracks. The Amtrak spur also includes coverage of the 1st Street Tunnel. The National Capital Region was chosen for the initial pilot program because of the location of the rail line, including its proximity to some of the Nation's most significant monuments and icons, as well as the U.S. Capitol. Recognizing the sensitivity surrounding rail infrastructure and freight traffic through large cities, as well as the unique security challenges presented by such an operation, this pilot project seeks to address security challenges while maintaining efficient rail operations.

IP has spent $15 million total on the NCRRPP. Ten million was funded for the CSX portion of the project from the Long Bridge to Benning Yard Rail Yard, and $5 million was funded for the Amtrak portion of the project from the 1st Street Spur, through the First Street Tunnel and Union Station to New York Avenue.

Question 12.: What steps has TSA taken to implement recommendations made by GAO in its September 2005 report on passenger rail security?

Recommendation 1: **Establish a timeline for completing the department's framework for analyzing sector risks and ensure that the risk assessment methodologies used by sector-specific agencies are consistent with this framework.**

The National Infrastructure Protection Plan (NIPP) establishes the risk assessment framework for the protection of critical infrastructure and key resources. The Transportation Sector Specific Plan (TSSP) has been prepared in a coordinated effort integrating Federal entities operating through Government Coordinating Councils (GCCs) with transportation stakeholders operating through Sector Coordinating Councils (SCCs). Modal annexes for passenger rail/mass transit and freight rail are being developed in a similar coordinated effort with the stakeholders in the respective modes. The risk management strategy for the TSSP and its modal annexes and for the National Strategy for Transportation Security aligns with the NIPP framework. The TSSP and modal annexes will specify timelines for risk analysis and other security priorities.

Recommendation 2: **a. Establish a plan for completing its methodology for conducting risk assessments that includes timelines and addresses how it will work with passenger rail stakeholders and leverage existing federal expertise in Department of Homeland Security components, including the Office for Domestic Preparedness, as well as the Department of Transportation modal administrations, including the Federal Railroad Administration and the Federal Transit Administration.**

At the operational level, the Transportation Security Administration (TSA) conducts security assessments under the Surface Transportation Security Inspection (STSI) Program. The purpose of assessing security status is to determine how individual operations compare to the baseline standards. Assessments in rail and passenger transit are conducted by TSA's field inspector force. The assessments are structured to target key areas of concern and to capture essential data to evaluate current practice versus baseline standards.

Passenger Rail and Mass Transit Status. The results of TSA's dual-track assessment initiative—STSI-led Baseline Assessment for Security Enhancement (BASE) reviews of security posture in the 17 Security and Emergency Management Action Items and the self-assessments by transit agencies on their posture in the 6 Transit Security Fundamentals—have indicated variations in security posture among passenger rail and mass transit agencies.

—To date, 48 of the top 50 agencies by passenger volume have completed the self-assessment and reporting the results to TSA. The reports show the agencies have taken these reviews seriously.
—The concurrent STSI-led effort has completed in depth BASE assessments on 34 of the top 50 agencies, focusing more deeply into the specifics of security plans and procedures, operational security activities, and programs for employee security training, drills and exercises, and public awareness.
—Additional assessments have been scheduled, with the objective of covering all of the top 50 agencies, then moving on to agencies ranked 51 through 100. TSA will complete assessments of the top 50 during fiscal year 2007 and initiate assessments on agencies ranked 51 through 100 during fiscal year 2007 for projected completion before mid–FY 2008.
—The data indicates varying security status among systems.
—The results are shaping TSA's strategic and operational security priorities, including security enhancement programs, grant funding, and engagement with individual passenger rail and mass transit agencies.
—Follow-on assessments will measure progress in improvement in the Actions Items and the fundamentals.

Freight Rail Status. To evaluate the security baseline in freight rail, TSA in cooperation with the rail industry is developing a comprehensive database driven system to identify the specific locations where toxic by inhalation (TIH) risk is the highest. TSA inspectors will verify attended/unattended status and proximity to high risk structures. In addition to identifying high risk locations, the database will give TSA the ability to identify TIH cars in near real time. This capability will allow us to more effectively respond to emerging threat situations.

Further, TSA inspectors have conducted field interviews with key rail management and personnel. Over 2,600 interviews have been completed, focused on employee security awareness, security procedures and systems to locate and protect TIH cars.

b. Evaluate whether the risk assessment methodology used by the Office for Domestic Preparedness should be leveraged to facilitate the completion of risk assessments for rail and other transportation modes.

To promote interagency coordination and information sharing on risk assessment activities and to bring the assessment methodologies within a consistent framework and leverage the existing methodologies, DHS, and its Federal partners have formed the Federal Risk Assessment Working Group, the Interagency Mass Transit Security Information Program, and the Risk Assessment Policy Group. These groups work together to coordinate Federal risk assessment activities and to promote consistency in risk assessment approaches. The former Office of Domestic Preparedness (since renamed the Office of Grants and Training, G&T) is a participant in these risk assessment coordination groups. G&T also participated in the development of the BASE program.

Recommendation 3: **a. Develop security standards that reflect industry best practices and can be measured, monitored, and enforced by Transportation Security Administration rail inspectors and, if appropriate, by rail asset owners. This could be accomplished by using the rule-making process, with notice in the Federal Register and an opportunity for interested stakeholders to comment, to promulgate long-term regulations that incorporate these standards.**

TSA is working closely with the Department of Transportation (DOT), other DHS components with transportation security responsibilities, and the transit and passenger rail industry to develop and disseminate the Security and Emergency Management Action Items, the Recommended Protective Measures for Homeland Security Advisory System (HSAS) Threat Levels, and the Transit Tunnels Security Action Items. Collectively, these security guidelines aim to elevate baseline security posture. Under the BASE program, STSIs assess transit agencies' implementation of these security measures.

The BASE program aims to elevate security generally and expand TSA's awareness and understanding of security posture in the passenger rail and mass transit mode. This information enables more effective targeting of security programs and technical assistance to elevate security. Through this process, TSA also identifies best security practices for sharing with the passenger rail and mass transit community, further enhancing security posture. The thorough review of security programs and procedures affords the systems assessed the opportunity to review the state of their security program and identify strengths and weaknesses. This information can guide the effective application of available security resources, focus collaborative ef-

forts with TSA, and facilitate the preparation of funding requests through security grant programs.

A key component of the strategic approach to passenger rail security is the development of security standards reflecting the combined expertise and experience of subject matter experts in the Federal government and the industry. The American Public Transportation Association (APTA) has initiated an effort to develop consensus on performance-based security standards for public transportation systems, including passenger rail. Federal participation in this effort will facilitate achievement of objectives articulated in section 3028 of the Safe, Accountable, Flexible, Efficient Transportation Equity Act—A Legacy for Users (SAFETEA–LU) Pub. L. 109–59) and in the Public Transportation Annex to the DHS/DOT Memorandum of Understanding(MOU) on transportation security. APTA seeks this participation. TSA is working with its Federal partners in the Transit, Commuter and Long Distance Rail Government Coordinating Council to engage in an effective manner that enables active involvement in the development of security standards and accords with applicable legal requirements. Adoption of the resulting standards by passenger rail systems would be evaluated by STSIs during assistance programs and inspections.

b. Set timelines for completing the memorandum of understanding modal agreements for rail, mass transit, and research and development, which both the Department of Homeland Security and the Department of Transportation have agreed to pursue.

All actions are completed. In September 2004, DHS and DOT executed a MOU to facilitate the development and deployment of transportation security measures. TSA, the Federal Transit Administration, the Office of Intelligence, Security and Emergency Response (S–60) in the Office of the Secretary/DOT, and DHS's Office of State and Local Government Coordination and Preparedness (SLGCP) and G&T have completed the Public Transportation Annex. In the freight rail mode, TSA joins the Federal Railroad Administration and the Pipeline and Hazardous Material Safety Administration in the Rail Security Annex, executed in 2006.

Recommendation 4: **a. 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 United States and abroad.**

Effective implementation and use of the Homeland Security Information Network is critical to the success of Federal information-sharing efforts. DHS established HSIN for stakeholders to use in the various Sector Coordinating Councils. The network includes a Public Transit Portal, intended for use as an information-sharing and exchange resource for transit systems throughout the country. An often expressed concern of transit system security officials is the absence of a single source or one stop shop for Federal information on transit security. The Public Transit Portal on HSIN has been developed to meet this purpose as the gateway to Federal information updates and resources for the mode and information and material developed by the Public Transit Information Sharing and Analysis Center. Feedback from mass transit and passenger rail systems will help ensure information products meet security needs. A concerted effort to populate the site with useful and timely information is ongoing.

A key component of the portal is the Mass Transit Resource Center. The Resource Center provides a comprehensive database for the transit industry to access information on a broad spectrum of subjects pertinent to transit security. This material is not readily available in a consolidated format elsewhere. TSA uses the Portal to provide timely security alerts, advisories, and information bulletins to passenger rail and mass transit agencies. Technology updates constitute an important component of this resource. Overall, the Resource Center covers more than 20 subject areas of security interest to the public transportation community, reflecting the feedback received from stakeholders on the type of information they require to meet the security mission.

Technology must be fully incorporated into the security operations of mass transit and passenger rail agencies. Presently, a variety of technologies are on the market or being tested, such as intrusion detection, video surveillance, anomaly detection, and chemical/biological/ radiological/nuclear detection. TSA, along with its public and private partners, is working to identify technology gaps and conduct research and development to provide technological solutions. The Federal partners are also harnessing the information gained from completed developmental testing and other use experience to provide the transit community a security technology information resource to guide procurement decisions. This resource will be a key component of the Public Transit Portal in the HSIN, meeting a specific requirement of Executive Order 13416, "Strengthening Surface Transportation Security."

b. Evaluate the potential benefits and applicability—as risk analyses warrant and as opportunities permit—of implementing covert testing processes to evaluate the effectiveness of rail system security personnel; implementing practices used by foreign rail operators that integrate security into infrastructure design; and implementing random searches or screening of passengers and their baggage, pending the results of an ongoing joint federal and industry review of the impact of random screening on passenger rail operators.

Security-oriented design considerations for infrastructure that assist the passenger rail industry to deter and minimize the effects of attacks on the entire rail passenger system are being evaluated by the DOT and TSA. DOT, working with industry representatives, has issued a report which offers security-oriented design considerations for transit infrastructure. There is also an effort underway by DOT to require vulnerability assessments on preliminary design plans for new public transportation projects including passenger rail. The Federal government provides training courses focused on effective design for security. The existing courses are "Transit System Security" and "Transit System Security Design Review." In development is a course that will be entitled, Transit Security Design Considerations.

Three transit agencies have instituted random bag inspection programs: the New York Metropolitan Transportation Authority, the Port Authority Trans–Hudson, and the Massachusetts Bay Transportation Authority. The decision to implement this type of program is best left to the individual transit agencies and their supporting law enforcement and security forces. The local officials are best placed to assess the advantages and drawbacks of this approach.

TSA provides assistance to transit agencies in security enhancement, regardless of the approach taken on this particular issue. TSA, in conjunction with the DHS Office of Science and Technology, advances the development and testing of security technologies suitable for the passenger rail and mass transit mode. To ensure technology enhances security capabilities in transit agencies, the Federal effort seeks development of mobile and fixed systems amenable to the demands of the transit environment that may be deployed flexibly for maximum deterrent effect and protection of high risk infrastructure. Pilot testing will employ equipment in this manner to validate capabilities most effectively. Future research and development initiatives will maintain this focus.

Through the Visible Intermodal Prevention and Response (VIPR) program, TSA deploys resources to supplement security activities of transit agencies. Deployments may consist of varying force packages of STSIs, Federal Air Marshals, explosives detection canine teams, and Transportation Security Officers, as well as necessary equipment, including security screening technologies. To enhance the capabilities and effectiveness of these deployments, TSA has procured screening technologies that are deployed and exercised in the passenger rail mode to develop concepts of operations specific to particular transit agencies. The resulting experience and operating procedures guide procurement decisions and operational use of screening equipment.

Covert testing has potential value as part of an overall security engagement approach with particular transit agencies. TSA has developed proposals for this activity. Coordination for testing with a particular system is ongoing.

On the international front, TSA engages extensively with its foreign counterparts on rail and transit security matters with the aim of sharing and gleaning effective practices for potential integration in the domestic strategic approach. TSA conducts and maintains these efforts in collaboration and coordination with the Department of State, DHS component agencies, and other Federal agencies on projects involving transportation security within international and regional organizations.

Engagement within the Group of 8 (G8) and with the European Union, the Asia Pacific Economic Cooperation, and the Mexican and Canadian governments fosters sharing of effective practices and technologies in mass transit and passenger rail security. The expanding cooperation in this area has culminated in creating an international working group on land transport security outside of any preexisting forum with preliminary focus on passenger rail and mass transit security. The United States will support this collaborative effort by providing information on most effective security practices and the effectiveness of security technologies.

TSA also participates in the Rail and Urban Transport Working Group in support of technology information-sharing across five countries. The membership of this group consists of the United States, United Kingdom, Canada, France, and Israel. In this forum, technology and operational experts come together to share information on technology testing and evaluation projects.

Through the Joint Contact Group, the United States and the United Kingdom engage in a bilateral cooperative effort to develop and promulgate best practices in rail

and mass transit security with the objective of developing security solutions applicable on a wider international basis. This group also explores opportunities to encourage broader private sector involvement in the protection of soft targets, such as through training of mass transit employees.

Another international initiative focuses on vetting suspicious packages detected in transit systems. This joint effort, involving TSA STSIs, Los Angeles law enforcement representatives, and British security officials, will bring training, experience, and lessons learned to the American participants from a British program known as Hidden and Obviously Typical (HOT) on suspicious packages. This program enhances the ability of the trained personnel to identify indicators of security concerns with packages left unattended in transit and rail facilities and vehicles.

TSA will continue a dynamic effort to engage with international counterparts, whether through bilateral arrangements or broader forums and working groups, and advance sharing of lessons learned and best practices to enhance security in passenger rail and mass transit systems.

Question 13.: Each mode of transportation presents its own risks. **How would you characterize the risks faced by passenger rail systems? How would you compare these with the risks faced by other modes of transportation? Is the current allocation of federal resources for rail security commensurate with the unique risks these systems face?**

Response: The Transportation Security Administration (TSA) takes a network approach to transportation security and views it as a shared responsibility. The responsibility and effort are shared among all of TSA; the Department of Homeland Security (DHS); other government agencies and entities at all levels, including Federal, State, local, tribal and territorial; and owner-operators.

The difference in Federal funding for aviation and surface transportation does not present the complete picture. Whereas Federal funding constitutes a substantial portion of aviation security monies, the Federal portion for surface transportation security constitutes a much smaller percentage of the total spent for surface transportation. When the money spent by private industry, states, and localities is added to the Federal portion, the total funds for surface transportation security are commensurate with the risk.

Much of the Nation's aviation infrastructure is federally owned. Surface modes of transportation are approximately 95 percent privately owned and operated. They receive security funding support from multiple streams (i.e., State, local, private, as well as Federal). The Department has consistently stated that responsibility for surface transportation security is a shared responsibility among a variety of stakeholders, including State, local, and Federal agencies, and private owners and operators. The appropriate role for the Federal government includes: using the substantial resources already in place and providing critical information; setting national priorities; developing transportation security fundamentals; coordinating ongoing efforts; and encouraging certain actions that reduce risk to the Nation's transportation system.

The bulk of Federal spending in aviation security has covered the compensation and benefits of Transportation Security Officers, who work every day in more than 450 airports nationwide to ensure the skies remain secure. Aviation security allows for point defense. We can seal off an area of the airport and only permit entry to those with tickets who have passed through screening.

The rail and mass transit modes do not allow for this type of approach. These systems operate over a broad geographic spread with numerous stations and transfer points providing the efficiency and fast-pace that are essential to moving thousands of passengers, particularly during daily rush hours. The point defense approach taken at the airports is neither practicable nor desirable. Rather, an integrated strategy, tapping the strengths of the Federal government, State and local governments, and passenger rail and mass transit agencies, must be pursued.

In evaluating the resources required to address surface transportation risk issues, it is important to take into account not just TSA's budget and statutory obligations in aviation, but also the substantial efforts, capabilities and expertise that already exist in the surface transportation environment, as well as very different operating, legal, and resource requirements. Therefore, the level of TSA's budget allocated to surface transportation security relative to aviation does not and cannot reflect the overall relative risk between them. In fact, TSA does give attention and priority to surface transportation, but TSA's role relative to the security partners in the networked approach is different than it is in aviation.

TSA has looked across all modes of transportation and set risk-based priorities. These priorities are used to focus TSA's attention and resources on those issues. TSA has conducted or participated in various risk analyses that compare risks

across different transportation modes, including most recently the DHS Strategic Homeland Infrastructure Risk Assessment (SHIRA). Surface transportation, transit and rail are currently high priorities for TSA. The level of funding is determined by the degree to which TSA can effectively mitigate the risks, as compared to the degree with which industry and other stakeholders are able to mitigate the risks.

For transit, a top priority is high density passenger transit systems in urban areas with underwater or underground tunnels. The risk of an improvised explosive device attack in a mass transit environment has been repeatedly demonstrated throughout the world, including London, Madrid, and India. As a result, TSA augmented its security efforts in Mass Transit to include: Visual Intermodal Protection and Response (VIPR) teams; bomb-sniffing dogs; assistance with training and managing system-owned explosive detecting canines; and a range of pilot and experimental screening, detection, and deterrence programs.

In addition, TSA is working to improve the risk basis for the Transportation Security Grant program. While the criteria for allocating grants among large transit systems continue to evolve, the criteria for approving specific project plans for actually spending the money is tightly focused on projects that mitigate prioritized risks.

Question 14.: Why did the President only request an additional $4 million for surface transportation security? Your surface transportation security budget is still less than 1% of your aviation budget.

Response: The Transportation Security Administration (TSA) supports the President's fiscal year (FY) 2008 budget request. The budget request accurately reflects the funding necessary to carry out different approaches to different modes of transportation.

The difference in Federal funding for aviation and surface transportation does not present the complete picture. Whereas Federal funding constitutes a substantial portion of aviation security monies, the Federal portion for surface transportation security constitutes a much smaller percentage of the total spent for surface transportation. When the money spent by private industry, states, and localities is added to the Federal portion, the total funds for surface transportation security are commensurate with the risk.

Much of the Nation's aviation infrastructure is federally owned, which requires a Federal budget. Surface modes of transportation are approximately 95 percent privately owned and operated, and receive security funding from multiple streams (i.e., State, local, private, as well as Federal). The Department has consistently stated that responsibility for surface transportation security is a shared responsibility among a variety of stakeholders, including State, local, and Federal agencies, and private owners and operators. The appropriate role for the Federal government includes: using the substantial resources already in place and providing critical information; setting national priorities; developing transportation security fundamentals; coordinating ongoing efforts; and encouraging certain actions that reduce risk to the Nation's transportation system.

The bulk of Federal spending in aviation security has covered the compensation and benefits of Transportation Security Officers, who work every day in more than 450 airports nationwide to ensure the skies remain secure. Aviation security allows for point defense. We can seal off an area of the airport and only permit entry to those with tickets who have passed through screening.

The rail and mass transit modes do not allow for this type of approach. These systems operate over a broad geographic spread with numerous stations and transfer points providing the efficiency and fast-pace that are essential to moving thousands of passengers, particularly during daily rush hours. The point defense approach taken at the airports is neither practicable nor desirable.Rather, an integrated strategy, tapping the strengths of the Federal government, State and local governments, and passenger rail and mass transit agencies, must be pursued.

Funding comparisons should also include:

—The commitment of Federal funds to intelligence activities to identify terrorists and detect their activities before they can present a threat or achieve their objectives;

— The commitment of Federal funds to capital improvements of passenger rail and mass transit systems that integrate security enhancements;

—The availability to transit agencies of 1 percent of Federal Transit Administration grants for training and exercises, approximately $40 million annually;

—The ability of States to allocate State Homeland Security Grant program funds to rail and transit system security;

—Direct grants to transit providers under the transit security and intercity bus security grant programs;

—The law enforcement agencies—either maintained by transit agencies or provided by State or local government—providing law enforcement and security services for passenger rail and mass transit systems operating within and/or through their respective jurisdictions; and

—Information sharing efforts that ensure security awareness is maintained at the Federal, State and local, and transit agency levels—such as the Public Transit portal of the Homeland Security Information Network that is maintained and operated at no cost to the transit community; the fee-funded Information Sharing and Analysis Center maintained by the American Public Transportation Association, now integrated into the Public Transit portal of the Homeland Security Information Network; and State and local intelligence fusion centers.

Federal funding contributes to all of these efforts, and will continue to do so, as part of a comprehensive, integrated strategic approach aligning the efforts of a range of entities and programs at the Federal, State, and local government and transit agency levels.

Question 15.: What is the role of funding in this issue (surface transportation security)? Is it a lack of funds or a lack of priorities on the part of the Department that is our biggest obstacle?

Response: The Department of Homeland Security's (DHS) priorities are well defined. The primary focus for DHS and the Transportation Security Administration (TSA) in mass transit and passenger rail has been information sharing, preparedness, domain awareness, training, and using a risk-based management approach to maximize the impact of available resources through random, visible security activities. One of the ways this is being done is through the transit security grant and intercity bus security grant programs. Through administration of these programs, TSA encourages potential grant applicants to submit project proposals that are aligned with national transportation security priorities. TSA is able to leverage grant funds to reduce risk by awarding grants to those projects that rank highest through evaluations based on:

- Funding priorities;
- Cost effectiveness;
- Ability to reduce risk of catastrophic events;
- Sustainability without additional Federal funds, combined with leveraging of other funding; and
- Ability to complete the project within the submitted timeframe.

TSA develops national priorities through system-wide risk assessments. Grant funds are awarded to transit systems that propose projects in alignment with national priorities and transit security fundamentals. The projects are implemented by transit systems often using additional private resources. Risk is reduced in those systems which also raises the level of security throughout the transportation sector.

Question 16.: What lessons can we learn from the attacks in Madrid, London, and Mumbai?

The London Underground's security efforts—use of CCTV, station design, training, etc.—are often cited as best practices. Despite these efforts, the system was successfully attacked. **What does this mean for other passenger rail systems? Can attacks not be prevented? If so, should we focus most of our efforts and dollars on response and recovery, rather than prevention?**

Response: Prevention is the highest priority for the Transportation Security Administration (TSA), and we take a layered, proactive, strategic approach rather than ceding to the terrorists by taking a reactive posture.

This approach starts by leveraging the work of other U.S. Government and allied foreign entities through effective gathering, analysis, and dissemination of intelligence and through information sharing.

The disruption of the terror plot in the United Kingdom in summer 2006 and other threats illustrates the necessity of this approach. The best defense is one that prevents the terrorists from ever entering the United States. Our aviation system security measures provide a significant barrier to entry for potential terrorists coming to our country. Our government's investments and improvements in terrorism watch lists, border security, and intelligence networks significantly enhance surface transportation security.

TSA complements these efforts by pursuing, as a strategic and operational priority, the expansion of visible, unpredictable deterrence environments in our surface transportation systems to disrupt terrorists' planning and preparation activities and execution of their missions. In securing transportation systems, we employ a network approach. While each transportation mode has its own security challenges, there are common vulnerabilities and mitigation strategies. In an effort to employ

the range of security resources most effectively, we work closely with transportation networks to leverage our security impact and determine risk-based priorities.

Building on this approach, TSA implements a comprehensive strategy that applies a common methodology across all transportation networks, regardless of mode. That strategy is straightforward. It consists of five elements:

- Assess industry threat, vulnerability, and consequence;
- Develop baseline security standards;
- Assess actual security status against baseline security standards;
- Develop plans to close gaps between actual status and baseline security standards; and
- Develop enhanced systems of security.

The top priorities in passenger rail security are encompassed within three guiding principles for the application of these elements:

- Focused effort to mitigate high consequence risk;
- Expanded employment of random, unpredictable deterrence; and
- Elevation of the security baseline through training, drills and exercises, and public awareness campaigns.

All of TSA's efforts—in development programs and resources to enhance and supplement security in rail and transit systems, in research and development of advanced security technologies, in deployment of Visual Intermodal Protection and Response teams—are driven by these priorities.

Question 17.: In 2005, the Government Accountability Office testified before the Senate Committee on Commerce, Science and Transportation that coordination between Departments of Homeland Security and Transportation could be improved, noting that the lack of coordination could lead to confusion, duplication, and gaps in preparedness. **Has coordination improved? What steps should be taken to further improve coordination?**

Response: Coordination between the Department of Homeland Security (DHS) and the Department of Transportation (DOT) on rail and transit security activities is strong. It is institutionalized in specific annexes to the DHS/DOT Memorandum of Understanding (September 2005). TSA and the Federal Transit Administration (FTA), along with the DHS Offices of State and Local Government Coordination and Grants and Training (G&T), have executed and implemented the Public Transportation Annex. In the freight rail mode, TSA joins the Federal Railroad Administration and the Pipeline and Hazardous Material Safety Administration in the Rail Security Annex.

These Federal agencies coordinate their activities under these agreements, as implemented through the Government Coordinating Councils and subject matter specific working groups. Regular consultations and meetings occur under these processes to ensure a coherent Federal approach to rail and mass transit security.

Recognizing the importance of information leadership, the Mass Transit and Passenger Rail Security Information Sharing Network has been fully established and information-sharing and communications protocols have been put in place. Participating entities include TSA's Mass Transit and Passenger Rail Division, Office of Intelligence, Office of Chief Counsel, and Public Affairs; DHS G&T, and State and local Government Coordination and the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC); and DOT's FTA. This Network ensures the timely dissemination of accurate information during normal operations and security incidents among Federal entities and with the passenger rail and mass transit community. Accompanying this network, the Homeland Security Information Network—Public Transit Portal (HSIN–PT) is being developed to facilitate communications among the transit community and the respective transit security related government agencies. The HSIN–PT officially launched earlier this year.

Further steps needed at this stage involve continuing to refine and enhance the existing procedures to maintain effective coordination on matters related to passenger rail and mass transit security.

Question 18.: Chris Kozub from the National Transit Institute (NTI) has testified before our Committee on training for mass transit employees. In his testimony, he stated that NTI and FTA's training had reached about 20% of the transit employee workforce which is approximated to be about 300,000. As of today that number has increased to slightly higher than 30%. While reaching 90,000 employees—many of whom are employed by the larger, security critical, metropolitan systems of the country—is a noteworthy accomplishment, NTI is still below the halfway point and has a lot of work still to do.

What steps have been taken to reach the remaining 70%?

Which agency is responsible ensuring that all employees receive training?

Response: Well-trained employees are a security force multiplier for security efforts implemented by transit agencies. The Transportation Security Administration (TSA) has set targeted counterterrorism training of front-line employees as a strategic priority, using the Transit Security Grant Program (TSGP) to provide transit agencies with the resources necessary to expand the scope and quality of training in their systems.

TSA, in coordination with the DHS Office of Grants & Training and the Federal Transit Administration (FTA), developed the Mass Transit Security Training Program, which identifies specific types of training at basic and follow-on levels for particular categories of transit employees. Presented in a readily understandable matrix, the Program provides effective guidance to transit agency officials in building and implementing training programs for employees working in their systems. To support execution of such training programs, the TSGP offers pre-packaged training options agencies may obtain with grant funding. Agencies taking advantage of this program have their applications expedited for approval to ensure funds are delivered within 90 days of submission. This initiative aims to expand significantly the volume and quality of training for transit employees during 2007. Thus far, 21 agencies have applied for training under this initiative among the Tier 2 systems alone for fiscal year (FY) 2007 TSGP funding. Nine other transit agencies proposed training in their standard fiscal year 2007 TSGP applications.

Which agency is responsible ensuring that all employees receive training?

Response: The Transportation Security Administration (TSA) has lead responsibility for ensuring transit agency employees receive security training. As is the case with all of our security programs, we execute this responsibility in coordination with our Federal partners. In security training, TSA and FTA jointly fund security training courses. Since 9/11, the 18 Federal security courses have been delivered more than 500 times reaching more than 90,000 transit employees. The Mass Transit Security Training Program, advanced by the expedited training application initiative under the TSGP, demonstrates TSA leadership in providing transit agencies with focused training guidance and the means to expand the scope and quality of training of their employees.

Question 19.: It is my understanding that as drafted the Notice of Proposed Rulemakings (NPRMs) recently released by TSA and the Department of Transportation will preclude state and local officials from mandating the rerouting of hazardous material. **Why did you include this provision in your NPRMs?**

Response: The Transportation Security Administration's (TSA) Rail Transportation Security Notice of Proposed Rulemaking does not address rerouting of trains. We cannot answer for the Department of Transportation.

Question 20.: Canine detection teams, which consist of a canine and a handler, are an important part of a layered homeland security system to prepare for, respond to, and prevent acts of terrorism. Canines can be trained to detect a variety of items, including explosives, narcotics, concealed humans, cadavers, and chemical and biological materials. Canine detection teams can be deployed quickly and can move easily throughout a variety of areas, including mass transit systems, airports, cargo areas, sea ports, the Nation's borders, ports of entry, office buildings, and stadiums. At our Full Committee hearing on February 9th, Secretary Chertoff testified the Department of Homeland Security "can't produce the dogs fast enough," and canines "are better than most technologies." Yet, we have a serious shortage of trained detection canines.

Could you please give us some examples of how TSA utilizes canine detection teams?

Response: The National Explosives Detection Canine Team Program (NEDCTP) deploys Transportation Security Administration (TSA)-certified explosives detection canine teams in the aviation and mass transit environments. The NEDCTP deploys a four-pronged approach in the aviation environment and a three-pronged approach in the mass transit environment. The aviation sector consists of cargo screening (national goal is 25 percent of the teams? overall utilization), Intensified Canine Patrol Strategies (ICPS) (random and unpredictable deployment of canine teams at curbside, check points, gate areas, terminals, etc.), pro-active searches (public visibility/deterrence), and response to threats. The mass transit sector consists primarily of ICPS, pro-active searches and response to threats.

Do you know approximately how many canine teams TSA currently has?

Response: TSA has 422 planned with 393 deployed teams in the aviation environment and 56 planned with 48 deployed teams in the mass transit environment.

These numbers change slightly on an ongoing basis, due to the addition of teams, retirement of canine, team performance issues, and handler assignments.

How many more does TSA need?
Response: The current base of funds will support 478 teams in fiscal year (FY) 2007, of which 422 are in aviation and 56 are in mass transit. The President's fiscal year 2008 budget will add $3.5 million for approximately 45 teams in the mass transit/maritime (ferry systems) environment. Although TSA receives requests for additional canine teams, it is difficult to gauge the overall need for teams on a national basis. The number of teams planned and deployed is in direct proportion to baseline funding levels.

Does TSA have a program to provide canines to state and local agencies?
Response: Yes.

If so, could you please describe it?
Response: The NEDCTP provides TSA-certified explosives detection canines to over 80 law enforcement agencies across the United States through a Cooperative Agreement. In addition, TSA provides partial reimbursement to these agencies to offset the deployment costs of these teams and to meet TSA security requirements outlined within the Cooperative Agreement. TSA also provides explosives detection canines to law enforcement agencies across the country through its National Breeding and Development Center. These are canines that are considered excess to the NEDCTP because they do not meet the program's rigorous standards but are adequate for use by State and local programs that have different requirements and training regimens.

How does TSA and its canine training programs work with the Office for Bombing Prevention within the Preparedness Directorate?
Response: The NEDCTP works in close partnership with the Office of Bombing Prevention (OBP) and collaborates with OBP on the Scientific Working Group for Dog and Orthogonal Detection Guidelines (SWGDOG). The NEDCTP has worked in concert with the OBP since its inception on issues such as training, performance standards, and deployment of highly skilled and qualified explosives detection canine resources.

I visited TSA's National Explosives Detection Canine Team Program and its Puppy Program in San Antonio, Texas, last August. **Does TSA plan to expand both of these programs to accommodate the need for additional canine detection teams?**
Response: Yes. Based upon funding levels in the out years, TSA plans to expand both the production of the National Breeding and Development Center (Puppy Program), and the training of canines and handlers at the National Explosives Detection Canine Training Center.

Both of these programs are co-located with the Department of Defense's canine training programs at Lackland Air Force Base. **Will this location permit the expansion of TSA's programs or will additional facilities be necessary?**
Response: On March 9, 2007, the Assistant Administrator—Office of Law Enforcement/Federal Air Marshal Service met with senior leadership at Lackland Air Force Base and discussed this issue. The current partnership in place with the Department of Defense will help facilitate NEDCTP infrastructure requirements at Lackland, and tentative plans are in place to facilitate future expansion.

Would you please discuss the resource-sharing arrangement between TSA and the Department of Defense with respect to canine training?
Response: Both the Department of Homeland Security (TSA) and the Department of Defense benefit from the current resource sharing arrangement. Facilities, resources, veterinarian care, lessons learned (Iraq/Afghanistan), canine resources, kennels, etc., are all shared. Each week, military canine handlers graduate in the same facilities as their TSA-sponsored civilian law enforcement counterparts, and representatives from each department are present at these graduation ceremonies. This cooperative working relationship between the two Departments results in the delivery of the highest level of security by providing valuable canine resources at home and abroad.

Are TSA-trained canines eligible to be transferred to another entity—Federal, state, or local—or sent overseas?
Response: Yes. Based upon our current agreements with the Department of Defense, canine assets are occasionally exchanged if they are not suitable for deployment in a transportation environment. In addition, canines that do not meet the

rigid selection standards put in place by the NEDCTP are often offered to Federal, State and local police departments to assist in fulfilling their canine requirements.

Question 21.: When TSA was originally formed shortly after September 11th, there was a Memorandum of Understanding between the Department of Defense and TSA regarding funding for the canine programs.

Response: The National Explosives Detection Canine Team Program (NEDCTP) has entered into what is called an Inter Service Support Agreement (ISSA) with the Department of Defense. This agreement has been in place since 1972, beginning with the legacy Federal Aviation Administration (FAA) canine program (formerly called the Canine Explosives Detection Team Program). During the transfer of NEDCTP functions from FAA to the Department of Homeland Security's Transportation Security Administration (TSA), this agreement was re-executed.

Is a revision to this agreement necessary?

Response: Not at this time. The agreement is currently being reviewed (Tri-annual Review) and is in the final coordination process within TSA.

WILLIAM W. MILLAR RESPONSES TO QUESTIONS FROM THE HONORABLE BENNIE G. THOMPSON

1. Your industry has continuously resisted mandatory security plans and vulnerability assessments, which will be required by this legislation. However, ports, the chemical industry, and the aviation industry all have to submit mandatory plans to DHS. **Why do you feel your industry should be excluded from this requirement?**

The public transportation industry has not resisted security plans and vulnerability assessments as suggested in this question. To the contrary, the industry fully supports continual security planning and the updating of assessments on a case-by-case as needed basis, determined through our continual work with federal, state, local, and on-staff security authorities. With respect to security plans, rail transit and commuter rail systems have had security plans in place as early as 1990. In 1995, 49 CFR part 659 required all rail transit agencies by regulation to have system safety and security plans developed. At this same time the nation's commuter rail systems engaged in a voluntary approach that also lead to the development of system safety security plans for those systems. We have on numerous occasions urged Congress to avoid a "one-size fits all" approach and to appreciate that, even under a risk based grant distribution mechanism, all public transportation systems may have needs, but not the same capacity to undertake strict, mandatory requirements as envisioned in the committee's legislation. All public transportation systems have limited operations budgets, constrained by their public nature. The majority of the public transportation systems that have significant security related concerns already have security plans and appropriate assessment documents in place. The industry fully supports continuing that planning and updating those assessments, but has concerns about the rigid structure of requirements set up within the legislation.

According to the GAO, the FRA has been focusing its efforts to improve rail safety, addressing issues such as human error, inspections, and rail track failure. It seems that the industry views safety as a bigger, more pressing concern than the risk of terrorism.

2. Is there a nexus between safety and security concerns? Where do those issues overlap and where to they diverge?

The transit industry has long acknowledged the connection between both safety and security. In fact, in testimony before Congress, APTA has noted that a dollar invested for security is also a dollar invested to enable transit to address all manners of hazards including natural disasters, operation incidents and security incidents. In many cases the procedures and technology that are used for security also enhances capabilities for addressing all manners of hazards.

3. What measures have been or can be implemented that serves both purposes of safety and security?

Examples of some measures that have been implemented include: standard operating procedures; training of employees; public outreach and engagement; technology tools such as Closed-circuit Televisions (CCTV's) and interoperable radio systems.

4. How have you determined the greatest risk of attack for your system? What is the greatest risk?

Our estimation of risk exposure comes to us through research and historical data through the Mineta Institute and the Government Accountability Office (GAO).

These sources indicate that public transit has been a primary focus of terrorist activity and that the primary means of terror has been through the use of improvised explosive devices.

5. Given the open nature of passenger rail systems—multiple access points, large crowds of people, and no barriers—can anything be done to protect these systems?

Yes a great deal can be done, and is being done, to increase the security for public transportation systems, the people who use these systems and employees who work in those systems. The openness of the systems does create unique challenges, and we acknowledge that the public transit agencies cannot be 100% secured. We recognize, however, that we have a responsibility to the American people to take practical efforts in providing a secure service and environment. All public transportation systems can and do make continuous improvements to the security, preparedness, and response capabilities that will increase the safety and security of the nations 10 billion public transportation riders and over 360,000 of public transportation employees, especially in the event of a successful act of terrorism.

The Port Authority of New York and New Jersey released a report recently that the PATH train tunnels the run under the Hudson River are more susceptible to attack then previously thought.

6. What steps are being taken to ensure the security of the tunnels in New York and elsewhere?

We respectfully suggest that the Port Authority of New York and New Jersey respond to this question.

7. How much money will it cost to ensure that these tunnels are secure and who should pay for these security upgrades?

We respectfully suggest that the Port Authority of New York and New Jersey respond to this question.

8. What is your response to criticism that the industry cannot be trusted to police itself?

We are unaware of claims that public transportation systems themselves "cannot be trusted to police themselves" as our systems already have security teams, police departments and other methods in place. Public transit agencies report to and are overseen by public boards, and as such are accountable to the public and political scrutiny. It is the position of the industry that we are not fully aware of the role and activities of the current team of federal rail inspectors, and as a result, we have questions regarding the benefits of drastic expansion of the available team of rail security inspectors. The industry would like to know more about the goals, objectives and activities of these inspectors and the systems themselves would be open to a greater level of coordination with appropriate transit agency specific security officials.

9. Doesn't the fact that since your members are in business to make money, there might be an incentive to cut corners on things like security from terrorist acts? Especially in light of the fact that the Administration doesn't seem to think rail security is priority?

Public transportation systems are not "in business to make money" as our systems are public in nature. The federal government has recognized this for decades and has provided federal assistance to U.S. public transit agencies. The top priority for all of APTA's transit agency members is the safety and security of their riders and their employees. The ability of our systems to make the necessary security improvements and provide for the security operations requirements is directly related to the availability of public funding.

TSA started working to secure the aviation system in late 2001; it was heavily criticized for not involving aviation stakeholders in its efforts. In response, TSA committed to taking steps to enhance its coordination with stakeholders in the future.

10. Is it your opinion that rail and mass transit stakeholders are appropriately involved as TSA moves forward with current and future security efforts, such as the recently issued proposed rule on rail?

TSA has existed for only the past five years, and as such their working relationship with the transit industry continues to be a work in progress. The transit industry looks forward to the development of a strong working relationship that includes the TSA's engagement of transit at the earliest stages of strategic planning.

11. TSA issued rail security directives in May 2004. What was the industry's reaction to these standards and how could they be improved?

Our view is that the industry led standards which involve full partnership with the TSA would be much more effective than the issuance of directives or regulations. It needs to be noted that mandates without appropriate funding are doomed for failure.

12. TSA continues to emphasize the importance of carriers identifying and reporting security risks to homeland security officials. Has your industry promoted whistleblower protections so that employees can report security concerns without fear of retaliation or retribution from employees?

Transit employees are largely covered under state laws for whistleblower protection. All 50 states have some form of state whistleblower protection laws, and transit employees are indeed covered under state law. Also, while transit employees are largely exempt from OSHA requirements, there are 26 state job safety and health plans that OSHA approves and monitors in which transit employees are covered.

13. TSA has recently issued a Notice of Proposed Rulemaking (NPRM) that would impose several new security requirements for rail carriers, rail transit systems; and rail operations at certain facilities that ship or receive hazardous materials. As part of this proposal, TSA would require rail and transit operators (as well as hazmat facilities) to allow physical inspection of their operations. In addition, chain of custody and hazmat tracking requirements will need to be enforced. **How many additional inspectors TSA inspectors do you anticipate will be needed for this expanded role?**

We believe that there would be greater benefit to the transit industry by directing funds to transit agencies rather than for additional inspectors.

14. Do you agree with the rule?

As stated in the previous answer, we believe that there would be greater benefits to the transit industry by directing funds to transit agencies rather than for additional inspectors.

15. What affect will this rule have on your industry as a result of real world implementation?

See above.

16. Will this rule improve security of hazmat transport?

The transit industry does not transport hazardous material.

17. It is my understanding that as drafted the Notice of Proposed Rulemakings (NPRMs) recently released by TSA and the Department of Transportation will preclude state and local officials from mandating the rerouting of hazardous material. This seems very favorable to industry and detrimental to security of our high population urban areas. **How can you justify this provision in the NPRMs?**

This question does not apply to the transit industry.

18. What do you feel is the carriers' role in providing security training for its employees?

We do provide security training for our employees, however, the transit industry is in need of appropriate funding levels to ensure that all employees are trained and on a regular and on-going basis.

19. Do you wish you had more guidance from DHS on this issue?

No, however, we do wish we had more federal funding from DHS to support security training.

20. Do you think TSA should mandate security training for mass transit employees?

We believe mandatory training without appropriate federal funding would be ineffective.

21. What are the costs of securing our rail and mass transit systems?

In 2004, APTA surveyed its U.S. transit agency members to determine what actions were needed to improve security for their customers, employees and facilities. In response to the survey, transit agencies around the country identified in excess of $6 billion in transit security investment needs.

22. How would you compare the risks facing the passenger rail systems with the risks faced by other modes of transportation? Is the current allocation of federal resources for rail security commensurate with the unique risks these systems face?

The GAO released a report several years ago which said "about one-third of terrorist attacks worldwide target transportation systems, and transit systems are the mode most commonly attacked." Since September 11, 2001, the federal government has spent over $24 billion on aviation security while has only allocated $549 million for transit security. Last year's attacks in Mumbai and the previous attacks in London and Madrid further highlight the need to strengthen security on public transit agencies in the U.S. and to do so without delay. While transit agencies are doing their part, we need the federal government to be a full partner in the fight against terrorism. The federal government needs to increase federal support for transit security improvements.

Chris Kozub from the National Transit Institute (NTI) has testified before our Committee on training for mass transit employees. In his testimony, he stated that NTI and FTA's training had reached about 20% of the transit employee workforce which is approximated to be about 300,000. As of today that number has increased to slightly higher than 30%. While reaching 90,000 employees—many of whom are employed by the larger, security critical, metropolitan systems of the country—is a noteworthy accomplishment, NTI is still below the halfway points and has a lot of work still to do.

23. Do you feel that this is adequate to give workers the tools they need to respond to or prevent a disaster?

APTA strongly supports the security training program being offered by the NTI. However, further security training needs will continue to evolve and will require appropriate funding support through the federal government.

24. Do you feel the Federal Government should be responsible for ensuring that all employees receive training?

The federal government should be responsible for providing federal funding so that all employees can receive training.

25. What are your thoughts in the utilization of security practices used by other countries?

The U.S. transit industry works very closely with our international colleagues in the sharing of information and effective practices. While there are many things we are learning through our international partners, there are many responses and measures being implemented in the U.S. that are of interest to our international partners.

26. With which practices were you most impressed?

Some examples of the practices and measures we were impressed with include behavioral assessment training; empowerment and training of the London underground personnel; operations control centers; and software advancements at the Metro Madrid.

27. Which do you think could be effectively implemented in the U.S.

Some of these initiatives are already being implemented. We believe with increased federal funding support all of the mentioned efforts could be implemented.

RESPONSES FROM EDWARD W. RODZWICZ

QUESTIONS FROM THE HONORABLE BENNIE G. THOMPSON

Question 1.: What has your organization done to raise awareness of your members and their employers to the security risk and to advance solutions and in-itiatives to enhance safety and security?

The Teamsters Rail Conference is proud to have undertaken a number of initiatives to raise awareness about security issues and to educate our members about this issue. For example, in 2005, the Rail Conference began an initiative known as "Safe Rails, Secure America," and conducted surveys of more than 4,000 railroad workers nationwide. The report which resulted from these surveys was entitled *"HIGH ALERT: Workers Warn of Security Gaps on Nation's Railroads."* The report details shocking inattention to security by the nation's largest rail corporations. We have distributed *High Alert* on a broad basis, and have reported extensively on the survey results in our internal communications media. In addition, we have worked with various media to educate and inform the general public of the need for safety and security improvements.

Also, along with a number of other organizations, Rail Conference constituents Brotherhood of Locomotive Engineers and Trainmen (BLET) and Brotherhood of Maintenance of Way Employes Division (BMWED) have sponsored hazardous materials training for more than a decade and a half at National Labor College, which is located at the George Meany Center in Silver Spring, Maryland.

Our Railway Workers Hazardous Materials Training Program (RWHMTP) has been a resounding success. The program has continually evolved and expanded to meet the training and competency needs of rail workers that are not met by the railroads. Initially offering only one course, the program now offers five, and training has moved beyond the conventional classroom to include simulation and on-line activities. A core of professionally trained instructors has been replaced with a corps of peer instructors. Because of this program's success, tens of thousands of rail workers are working more safely and in safer environments.

The RWHMTP has trained more than 20,000 rail workers, and the National Institute for Environmental Health Sciences-funded program now offers five courses: a five-day Chemical/Emergency Response training in the classroom; an on-line Emergency Responder Awareness Level 101 course; the OSHA 10-hour General Industry Safety and Health Outreach Program; disaster site training; and the newest addition, a Radioactive Material Transportation Safety Program, which is funded by a separate grant from the U.S. Department of Energy.

The newest program began last, and includes a Modular Emergency Response Radiological Transportation Training (MERRTT)"train the trainer" course. By contrast, we are unaware of any railroad currently conducting training focusing on transportation of spent nuclear fuel and high-level radioactive waste, even though the Department of Energy is expected to begin a 38-year project to transport such waste from DOE sites to storage and disposal facilities as early as next year. The labor hazmat program has trained workers in 49 states and the District of Columbia.

We also have fostered the creation of community partnerships that include joint rail worker, fire fighter, EMT, and public safety personnel training in communities throughout the U.S.

The program also includes an emphasis on railroad security and disaster response and teaches the five-day students how to serve as skilled support personnel in an incident command emergency setting. Much of the program material is available in Spanish and a comprehensive web site serves both the English and the Spanish-speaking work forces. The five-day program addresses the training requirements of the Department of Transportation's Hazardous Materials Regulations at 49 CFR Part 172, as well as the requirements of OSHA First Responder and Operations Level training under 29 CFR Part 1910.120. Railroads generally do not provide wages or support for workers attending the program. In fact—and this is most unfortunate—members sometimes are not allowed time off from work to attend the program, even though the railroad is not paying wages.

The program currently serves eight rail unions, and at least ten crafts, from major railroads as well as from commuter and short-line railroads. This cross-company, cross-union, cross-craft training has proved invaluable, as one group learns from another. Each union has its own craft-specific tasks and challenges, and prior to this hazmat training program there was little, if any, cross-union training. Hazards and challenges faced by those in the yards may be different than those faced by road train crews, and different still from those who work along the track or in the shops.

Understanding the work of other crafts, the safety and health challenges that each face, and the coordination of each craft's efforts in an emergency, enhances railroad hazardous materials safety and security. A well-trained and knowledgeable workforce is the first line of defense and can prevent a minor incident from becoming a major hazardous materials accident. The eight rail unions have worked together to enhance rail safety by providing comprehensive training to its members and by providing substantial administrative and personnel support to the union-run Railway Workers Hazardous Materials Training Program.

Labor has been able to offer these programs through a combination of federal funds and subsidies from the North American Railway Foundation, which is a private non-profit organization. However, subsidies and contributions are hard to come by. Nonetheless, we take great pride in having trained over 20,000 railroad workers since the program's inception, and we hope that H.R. 1401 will enable us to broaden the program offered by the RWHMTP. At the end of the day, though, this represents but a small fraction of the railroad workers who require thorough, in-depth training, and recurrent training.

Question 2.: The Chlorine Institute has estimated that a 90-ton rail tank car, if targeted by an explosive device, could create a toxic cloud 40 miles long and 10 miles wide. Such a cloud, according to U.S. Naval Research Laboratory, could kill 100,000 people in 30 minutes in a major metropolitan area.

Are our frontline workers able to handle an attack of that nature today?

We believe that they are not. To demonstrate the lack of preparedness, one need look no further than the tragedy that befell Graniteville, South Carolina, on January 6, 2005, when a moving Norfolk Southern train struck a standing train. While

no explosion was involved in Graniteville, the collision forces caused a tank car containing chlorine to breach, releasing chlorine gas. *See* NTSB/RAR–05/04 at p. v. The chlorine gas release caused the death of nine—including the train's engineer, BLET member Chris Seeling—and injured over 550 others, including 74 who were admitted to hospitals. *Id.* A hazardous materials team was not requested until seven minutes after the accident occurred, and only after the fire chief arrived at the scene. *Id.* at p. 13. A properly trained crew may have made such a request more quickly, and the casualties might have been reduced.

Question 3.: If not, why not?

Worker training still has not been given the attention that it deserves. The industry simply does not devote sufficient resources either to providing initial training for new workers or for periodic recurrent training to freshen the knowledge and skills of veteran workers. Far too often, training schedules are dictated by the need to deploy new workers in the field, rather than ensuring that those workers, and their more senior co-workers, have the necessary tools and skills set to work safely and efficiently. This long-standing trend has only been exacerbated by the retirement of the Baby Boomer generation of railroad workers, which is now underway.

Question 4.: What can be done to get them prepared?

Industry inaction over the past 5° years establishes beyond serious question that Congress must pass legislation to compel rail corporations to train their workers on proper safety and evacuation procedures; the use of appropriate emergency escape apparatus; the special handling of hazardous materials; and the roles and responsibilities of railroad workers within the railroad's security plans, including an understanding of the plan's threat level index and notification to the appropriate workforce segment each time the threat level is changed.

Question 5.: What do you see as the biggest security lapse in our freight/passenger rail systems?

The biggest lapses have occurred in worker training, and access to rail lines and yards, as demonstrated in the *High Alert* report.

You have been critical of industry for focusing too much on technology for security and not focusing on training of frontline employees. **But isn't technology important? What do you feel is the right balance between technological and human resources as it pertains to security?**

Technology can provide much value in security, but only within reasonable limits. Frankly speaking, the railroad industry only becomes excited with technology when it can be deployed in such a way as to reduce labor costs by automating some procedure currently performed by a human being, thereby enabling the railroad to eliminate jobs. Adopting such an approach with respect to security technology would be a waste of precious resources with precious little in return.

As we have seen through overreliance on technology in the intelligence sector and its failures, there are some things that human beings are better suited to do. Another example—perhaps better suited to rail security considerations—is the extent to which video cameras can enhance security. All of the terrorists who struck the London Underground in the July 7, 2005 attack were recorded on surveillance cameras; however, the existence of that technology did nothing to prevent the carnage. Even with optimal use of technology to enhance safety, which we support, railroad workers will continue to be the eyes and ears when it comes to security on the nation's railroads. Neither the industry nor the nation can afford to overlook these workers, because continuing to deny the resources necessary to train them leaves us all in a more vulnerable position.

Question 6.: In what areas would your members like to have more training with re-gards to security? Have you brought these concerns to the industry? If so, what was the response?

Training has been horribly inadequate in all areas. Locomotive engineers, trainmen and track maintenance workers are the true first responders to rail emergencies—the eyes and ears of the industry. They are the first on the scene, and often the last to leave. Yet, the rail corporations do not have quality safety and security training in place. That failure places these first responders in harm's way, and by extension puts the communities served by the railroads in harm's way as well.

Even since 9/11 and the attacks on rail and transit systems overseas, the security training given to rail employees has been minimal, usually comprised of nothing more than a printed brochure or 10-minute videotape. The shocking findings of the High Alert report identified in Question #1 above include the following:

- 94% of respondents said that rail yard access was not secure;
- 70% of respondents reported seeing trespassers in the yard; and

• only minimal security training had been provided to employees who have been warned that they could be the targets of a terrorist attack.

We have voiced our concern in every conceivable venue and at every possible opportunity, also as indicated in our response to Question #1. The industry's initial response was to claim that *High Alert* was nothing more than a propaganda piece issued in support of our collective bargaining goals. In more recent times, the industry has simply ignored our message, except to chant over and over—as if a mantra—that substantive training is being provided. However, the industry has yet to back up its claims with data or documents.

Question 7.: You note in your testimony "attempts" by TSA and FTA to establish se-curity training programs for employees. Yet you go on to say that de-spite these efforts, there still is no real, comprehensive, security training in place. **How do you account for TSA's reluctance to put forth a com-prehensive, standardized security training program? Why do you think rail and mass transit security is not yet a true priority for DHS?**

Considering the manner in which the 9/11 attacks were launched, it was reasonable for the federal government to focus on securing the commercial aviation industry. However, as aviation security was enhanced, no increased focus on rail and transit was evident until recently, and expenditure levels since 2001 have remained disproportionately aviation-targeted. For example, in 2006, the federal government spent $4.7 billion for airline security but only $136 million for rail and transit. To be certain, the industry's constant unsupported claims that security and preparedness could not be better have contributed to the general atmosphere. Interestingly, however, several months ago—when TSA and the Pipeline and Hazardous Materials Safety Administration proposed security regulations that included a requirement under which a railroad must be able to provide the location of a car carrying certain types of hazardous materials within one hour from a TSA request, the industry howled in protest. We believe the action taken by the House on rail security in this session is an excellent first step in putting us on the right track.

Question 8.: Do you think that TSA should mandate security training for frontline rail and mass transit employees?

Yes, security training for railroad workers should be federally mandated, so that it is consistent throughout the railroad and transit industries. The similar vulnerabilities between the industries—as well as within each industry—places essentially the same burden on Rail Conference members and other front line railroad workers

Question 9.: As TSA started working to secure the aviation system in late 2001, it was heavily criticized for not involving aviation stakeholders in its efforts. In response, TSA committed to taking steps to enhance its coordination with stakeholders in the future.

What steps is TSA taking to ensure that Labor organizations are part of this process? It is my understanding that TSA has not reached out to labor organizations representing the millions of men and women who are literally the eyes and ears of the rail and mass transit systems.

We have seen very little in the way of attempts by the TSA to ensure that rail labor is a part of the process. TSA does not regularly communicate with opportunities for input afforded us for more than a year and a half are public comment periods mandated by the Administrative Procedures Act.

Question 10.: What are the top three security practices used in other countries that you would like to see vetted here in the U.S. In your opinion, what are the obstacles to have those practices adopted here?

It is difficult to answer this question. Rail systems are especially vulnerable to terrorist attacks. I think that because railroads in other countries have directly experienced attacks, they may know better how to respond to them. However, I think the nature of railroads everywhere is that they are widespread and difficult to protect from attacks.

According to a GAO report on the subject entitled, "Passenger Rail Security, Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts," some foreign rail operators use testing and simulations to help keep employees alert to security threats or randomly screen passengers. Centralized clearinghouses on rail security technologies, such as chemical sensors, and best practices are also maintained in some foreign countries, and we would do well to become part of that network if we have not already done so. Application of measures used in other countries may pose challenges in the U.S. but they may be worth looking into, at the very least.

Question 11.: In the event of an attack, the people on the scene, the front-line employees, are critical to minimizing loss of life in the event of an emergency. They are called to recognize threats as well as respond to them.

Workers are critical as the first responders to railroad accidents, which is why the lack of training is especially outrageous. Locomotive engineers, trainmen and track maintenance workers are the true first responders to rail emergencies—the eyes and ears of the industry. They are the first on the scene, and often the last to leave. Yet, the rail corporations do not have quality safety and security training for their workers in place. That failure places these first responders in harm's way, and by extension puts the communities served by the railroads in harm's way as well.

Question 12.: Which systems are getting it right?

Because there has been no successful attack on any domestic rail freight, passenger, commuter or transit system since 9/11, we suspect that the industries would claim that they all are "getting it right." Unfortunately, in the absence of a rigorous program of training and simulation, there will be no way to know who is getting it right until an attack is attempted. Therefore, the Rail Conference doesn't believe that any railroad can claim such an achievement.

Question 13.: Who are the shining stars of employee training?

We believe that no railroad can make such a claim at this time.

Question 14.: What weight does your organization put on hazmat training?

We put a great deal of weight on hazmat training. As stated in response to Question #1, the Teamster Rail Conference, through its divisions, has long participated in the programs run by the National Labor College. These programs have been an integral part of our education and training of our members for many years.

Question 15.: Chris Kozub from the National Transit Institute (NTI) has testified before our Committee on training for mass transit employees. In his testimony, he stated that NTI and FTA's training had reached about 20% of the transit employee workforce which is approximated to be about 300,000. As of to-day that number has increased to slightly higher than 30%. While reaching 90,000 employees—many of whom are employed by the larger, security critical, metropolitan systems of the country—is a noteworthy accom-plishment, NTI is still below the halfway point and has a lot of work still to do.

15. Do you feel that this is adequate to give workers the tools they need to respond to or prevent a disaster?

Considering the fact that this figure does not include railroad workers, 30 percent is not enough. All workers who are on the front lines deserve to have the training they need to respond to incidents. Each weekday, 11.3 million passengers in 35 metropolitan areas and 22 states use some form of rail or mass transit. These passengers ride on trains that cover over 10,000 miles of commuter and urban rail lines. The very nature of the rail system makes it vulnerable to attack. In addition to the more than 10,000 miles of commuter and urban rail lines, there are 300,000 miles of freight rail lines. These lines are open and easily accessible to the general public. If an incident should occur, the workers will be the first to respond to it—and they need training in order to be able to do so.

Question 16.: Do you feel that the Federal Government should be responsible for en-suring that all employees receive training?

The federal government should mandate training for all railroad employees, whether it is supervised by the government and administered by the railroads or simply administered by the government—it needs to be done, and done this year.

TERRY ROSAPEP RESPONSES TO QUESTIONS FROM THE HON. BENNIE G. THOMPSON

Question 1.: What proactive measures has the Administration taken to prevent terrorist attacks to mass transit and rail infrastructure?

Mr. Rosapep: The Department of Homeland Security (DHS) and its Transportation Security Administration (TSA) have primary responsibility for transportation security, with the Federal Transit Administration (FTA) and the Federal Railroad Administration (FRA) providing support in the transit sector and with FRA, FTA, and the Pipeline and Hazardous Materials Safety Administration (PHMSA) providing support in the railroad sector. I will focus first on FRA's role and then on FTA's role in these security efforts.

FRA's involvement in railroad security predates the terrorist attacks on September 11, 2001. From October 1995 (when a deliberate act of vandalism caused a fatal Amtrak derailment near Hyder, Arizona) through March 2006 (when the USA

PATRIOT Improvement and Reauthorization Act of 2005 was enacted), FRA helped develop, and worked with Congress to secure the enactment of, Federal criminal legislation to deter and punish more effectively terrorist attacks against railroads and mass transportation systems. *See* 18 U.S.C. § 1992.

Since 9/11, FRA has been actively engaged in the railroad industry's response to the terrorist threat. 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, which permits timely distribution of information and intelligence on security issues. Working with FTA, FRA has participated in security risk assessments on commuter railroads, and FRA has conducted security risk assessments of Amtrak as well. FRA and PHMSA also assisted TSA in conducting risk assessments of rail corridors carrying high quantities of toxic inhalation hazard materials, helping negotiate the 27 security action items that the railroads have voluntarily agreed to implement, and in the development of the recently issued TSA notice of proposed rulemaking (NPRM) to ensure secure handoffs of dangerous hazardous materials in high threat urban areas. FRA also assisted in the development of the recently issued PHMSA NPRM that would strengthen the railroads' hazardous materials security plans. FRA's security director works on a daily basis with government agencies and the railroad industry to facilitate communications on security issues, and also participates in security training, reviews security plans, and performs other activities to promote rail security. For example, in 2007, FRA intends to conduct at least 15 security training sessions for rail labor organizations, as well as four sessions at the FBI Academy on railroad security and emergency response for law enforcement personnel. FRA is also conducting various research and development that will improve the safety and security of railroad operations.

With respect to FTA's role in transportation security efforts, that agency developed and launched a set of transit industry security initiatives, including the following:

—readiness assessments at 37 of the largest transit agencies (FRA partnered with FTA on four of these assessments conducted at commuter rail agencies.);
—drill and exercise grants offered to the 100 largest transit agencies;
—Connecting Communities Security and Emergency Management Regional Workshops held at 18 regions across the country;
—on-site security and emergency management technical assistance provided to the 50 largest transit agencies;
—funding improvements in intelligence and information sharing activities, such as the creation of the Public Transportation Information Sharing & Analysis Center (PT–ISAC);
—expanding the transit industry security training curriculum by developing and distributing specific new counter
-terrorism training courses;
—establishing and sponsoring semi
-annual Security Roundtables to facilitate peer-to-peer information sharing among the security chiefs at the 50 largest transit agencies;
—developing a Top 20 security action items baseline assessment tool and using it to identify and prioritize the development of industry guidance products to address any deficiencies;
—partnering with key industry stakeholders to develop and distribute an industry-wide "eyes & ears" campaign known as Transit Watch; and
—establishing and increasing international informational networks to identify lessons learned, best practices, etc.

With the creation of DHS (and the designation of TSA as the agency with responsibility for transportation security and the Office of Grants and Training (G&T) responsible for administering the transit security grant program), FTA has collaborated closely with DHS on transitioning its initial set of security initiatives to a Federal level partnership approach, per the terms of the DHS/DOT MOU Annex for Public Transportation Security. (Please see the response to Question 6, below, for more on the MOU Annex.)

Coordination among FTA, TSA, and G&T has helped solidify the transit industry focus on three strategic security priorities:

—security training for transit employees;
—public awareness (such as the Transit Watch campaign); and
—emergency preparedness.

Question 2.: Each mode of transportation presents its own risks. How would you characterize the risks faced by passenger rail systems? How would you compare these with the risks faced by other modes of transportation? Is the current alloca-

tion of Federal resources for rail security commensurate with the unique risks these systems face?

Mr. Rosapep: FRA works with and supports DHS, which has the lead on transportation security matters and may be able to provide additional information on this subject. FRA provided input for the National Infrastructure Protection Plan, which describes these risks in greater detail, compares the risks to which the various modes are exposed, and discusses matters pertinent to the available resources. In general, it should be noted that Amtrak, the Alaska Railroad Corporation, and commuter railroads provide passenger rail service to more than 500 million passengers yearly. Passenger operators face many challenges in their efforts to provide a secure public transportation environment. By definition, the systems are open, providing numerous points of access and egress, leading to high passenger turnover and making them difficult to monitor effectively. Amtrak, for example, operates as many as 300 trains per day serving over 500 stations in 46 States, and Amtrak trains use tracks owned by freight railroads except for operations in the Northeast Corridor and in Michigan.

Question 3.: What methods are being used to analyze and characterize the nature of various risks to rail and other modes of surface transportation?

Mr. Rosapep: In the first few years after 9/11, FRA participated with FTA in security risk assessments on the ten largest commuter railroads and contributed the funding for security risk assessments on three of these railroads. In addition, FRA participated in FTA's "best practices tool kit" initiative, contributing its knowledge of commuter rail operations, infrastructure, and organization to ensure that the recommended security enhancement measures were sound and feasible in a railroad environment. FRA staff continues to work closely with many of the railroads that receive FTA grant funding, to plan and assist in the development and implementation of security simulations and drills. Since the establishment of DHS, FRA has worked closely with and supported DHS in its leadership role on transportation security matters. As a general matter, in addition to the specific items discussed in these answers, FRA also devotes staff with both railroad knowledge and facilitation skills to the FTA—and TSA-sponsored workshops across the country (called "Connecting Communities") to bring together commuter railroads, emergency responders, and State and local government leaders so that they might better coordinate their security plans and emergency response efforts. DHS may be able to provide additional information on this subject.

Risk assessments are the primary analytical tool used by transit agencies to measure, quantify and prioritize relative risks to their people, operations and infrastructure. The dimensions of these risk assessments include threats, vulnerabilities and consequences.

The guidance that FTA and TSA provide to transit agencies regarding conducting risk assessments is as follows:

—establish a risk management process that is based on a system
-wide assessment of risks and obtain management approval of this process;
—ensure proper training of management and staff responsible for managing the risk assessment process;
—update the system
-wide risk assessment whenever a new asset/facility is added or modified, and when conditions warrant (e.g., changes in threats or intelligence);
—use the risk assessment process to prioritize security investments; and
—coordinate with regional security partners, including Federal, State, and local governments and entities with shared infrastructure (example: other transit agencies or rail systems), to leverage resources and experience for conducting risk assessments.

Question 4.: Why did President Bush only request an additional $4 million for surface transportation security? Your surface transportation security budget is still less than 1% of your aviation budget.

Mr. Rosapep: This question refers to the DHS budget, and the response should come from DHS.

Question 5.: What lessons can we learn from the attacks in Madrid, London and Mumbai?

a. The London Underground's security efforts—use of CCTV, station design, training, etc.—are often cited as best practices. Despite these efforts, the system was successfully attacked. What does this mean for other passenger rail systems? Can attacks be prevented? If so, should we focus most

of our efforts and dollars on response and recovery, rather than prevention?

Mr. Rosapep: We cannot guarantee that all terrorist attacks on transit can be prevented. However, some terrorist attacks have been prevented, primarily through effective intelligence—specific, timely analytical information that is shared with the appropriate authorities responsible for acting upon the information. The key is establishing and sustaining a comprehensive, balanced approach to transit security ? prevention, deterrence, mitigation, and response/recovery.

Some specific lessons learned:

Madrid: It underscores the important need for an "Eyes & Ears" campaign, like Transit Watch, and security awareness training for transit employees, to increase the odds of terrorists being detected during their casing/rehearsal activities.

[London: Most of the casualties occurred at the London Underground station with tight clearances between the tunnel and the rail cars, such that most of the blast pattern effects of the improvised explosive device had nowhere to go but back into the railcars. While retrofitting/hardening very old infrastructure may be very challenging and expensive, this highlights the importance of mitigating terrorist attacks through security design.

Mumbai: Planning of these attacks may have been aided by inside workers, emphasizing the importance of conducting background checks on employees, contractors, vendors, and others.

Question 6.: In 2005, the Government Accountability Office testified before the Senate Committee on Commerce, Science, and Transportation that coordination between the Departments of Homeland Security and Transportation could be improved, noting the lack of coordination could lead to confusion, duplication, and gaps in preparedness. **Has coordination improved? What steps should be taken to further improve coordination?**

Mr. Rosapep: 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 primary responsibility for security in all modes of transportation, but also recognizes that DOT plays a supporting role, providing technical assistance and assisting DHS when possible with the implementation of its security policies. The MOU reflects the agencies' shared commitment to a systems risk-based approach and to development of practical solutions, recognizing that each agency brings core competencies, legal authorities, resources, and expertise to the railroad transportation mission. The MOU requires early coordination between the parties on the development of regulations affecting security. Separate annexes have been signed concerning the implementation of the Homeland Security Council's recommendations concerning toxic inhalation hazard materials, and concerning the day-to-day coordination between FRA and TSA, among FTA, TSA, and DHS's G&T, and between PHMSA and TSA on security matters.

For example, the FRA–TSA annex provides for close cooperation between the two agencies on their programs and activities, including regulations affecting railroad security, legislation, research and development, inspection activities, and the response to threats to railroad security in order to maximize passenger and freight railroad security while minimizing disruptions to railroad operations to the extent practicable. The agreement provides that if an FRA inspector observes a significant security issue, the information will be provided to TSA and the railroad; similarly, if a TSA inspector observes a significant rail safety issue, the information will be provided to FRA and the railroad. FRA has one full-time employee addressing rail security matters, and all of FRA's 71 hazardous material inspectors and specialists, along with 17 State inspectors, devote a portion of their time to reviewing railroad and rail shipper security plans for compliance with PHMSA's hazardous materials security regulations.

While TSA inspectors have lead authority and responsibility in conducting security inspections and reviews, the interagency MOU does permit the use of FRA inspectors to support TSA's security efforts. FRA inspectors have conducted basic security reviews of Amtrak and commuter railroad security both after the 2004 train bombings in Madrid and after the 2005 transit bombings in London. In both cases, FRA inspectors were deployed immediately after the bombings to assess the security posture 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 rail security inspectors. TSA focused primarily on urban rapid transit lines, while FRA inspectors concentrated on commuter and intercity rail passenger operations; in some situations, inspectors from the two agencies worked jointly. FRA will continue to support TSA in responding to rail security threats.

FRA, FTA, and PHMSA have assisted DHS and TSA in the preparation of the National Infrastructure Protection Plan issued in June 2006, and have actively supported DHS and TSA's efforts to develop Sector-Specific Plans for critical infrastructure protection, as required by Executive Order 13416. I have previously noted how the three agencies have worked closely together on hazardous materials corridor risk assessments, assisting the railroads in adopting security best practices (known as security action items) for the transportation of certain hazardous materials, and developing NPRMS dealing with railroad hazardous material security. FRA has added TSA as a member of FRA's Railroad Safety Advisory Committee, the group that assists FRA in developing its safety regulations, in order to ensure that FRA's regulations advance both rail safety and security. From the time that DHS was created, FRA and TSA realized that close coordination was essential due to the great overlap between safety and security, and the two agencies have worked closely together since then. The close relationship of TSA, FRA, and PHMSA is reflected in the two recently issued, coordinated NPRMs to enhance the security of rail transportation.

FRA will continue to support DHS in carrying out its security responsibilities, and work with the rail industry to secure the Nation's freight and passenger railroad network. Together, DOT, DHS, and the rail industry are helping to ensure that security initiatives and programs are directed at potential threats to the Nation's railroad network and that rail employees and others responsible for its security are prepared to identify and address such threats.

The Annex agreed to by FTA, TSA, and G&T stipulates that these agencies have a mutual interest in ensuring coordinated, consistent, and effective activities that have the potential to materially affect the missions of both departments and sets out to delineate clear lines of authority and responsibility between the parties for transit security. Pursuant to this annex, DOT and DHS agreed to coordinate their programs and services, including training; awareness programs; emergency preparedness; security forums; information sharing; drills and exercises; risk assessment and reviews; technical assistance; research and technology; security standards; transit security grants programs; and interoperable communication. The Annex also stipulates that the FTA, TSA, and G&T will establish and implement an annual plan that will coordinate their transit security programs.

In support of the MOU Annex implementation, eight working groups have been established under an Executive Steering Committee comprised of leadership representatives from TSA, FTA and G&T to provide for coordination of public transit security programs as identified and agreed to in the Annex. These working groups are being integrated into the Transit, Commuter and Long Distance Rail Government Coordinating Council to facilitate engagement as necessary with the Mass Transit Sector Coordinating Council under the Critical Infrastructure Protection Advisory Council process. As part of its efforts to coordinate the programs of the participating agencies, the Executive Steering Committee is also responsible for identifying emerging needs in public transportation security and making coordinated policy recommendations to the leadership of each agency.

The Executive Steering Committee established the following project management teams:

- Assessments & Technical Assistance
- Standards & Research
- Transit Watch & Connecting Communities
- Transit Safety & Security Roundtables
- National Resource Center
- Training
- Annual Plan, Regional Transit Security Strategies and Grants
- Emergency Drills/Exercises

Question 7.: Do you think TSA should mandate security training for mass transit employees?

Mr. Rosapep: If transit agencies are mandated to conduct various training courses, many of them may strive for that minimum and not go above and beyond what may be desirable. We need to recognize and applaud the great strides that transit agencies have taken to incorporate training into their security programs and provide additional opportunities that allow them to take advantage of the existing offerings. Historically, the transit industry has been extremely receptive to guidance from the Federal government. The Federal government, therefore, should concentrate its resources on continued guidance and provide the resources necessary for transit agencies to take advantage of the existing and future offerings.

According to the GAO, the FRA has been focusing its efforts to improve rail safety, addressing issues such as human error, inspections, and rail track failures. It

seems that the industry views safety as a bigger, more pressing concern than the risk of terrorism.

Question 8.: Is there a nexus between safety and security concerns? Where do those issues overlap and where do they diverge?

Mr. Rosapep: Rail safety and security are interrelated. 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. FRA's railroad safety mission necessarily includes its involvement in railroad security issues. As previously stated, DHS and its TSA have primary responsibility for transportation security, with FRA, FTA, and PHMSA providing support in the railroad sector. FRA works closely with TSA and the railroad industry on a daily basis in addressing railroad safety issues that involve security, participates in the Government Coordinating Council for Rail, and contributes its expertise to the implementation of Executive Order 13416, "Strengthening Surface Transportation Security," including providing input for the National Infrastructure Protection Plan and Sector Specific Plans, as well as the National Strategy for Transportation Security.

While FRA's rules are focused on the safety of railroad operations, they necessarily have some bearing on security. For example, Federal passenger and freight equipment standards are intended to ensure that the equipment can withstand forces of derailments and collisions, whether caused by accidents or deliberate acts, thereby helping to protect passengers, employees, and surrounding communities. PHMSA's December 21, 2006 NPRM on rail security proposes changes to the Hazardous Materials Regulations that would require rail carriers to inspect tank cars carrying hazardous material for the presence of improvised explosive devices or other suspicious objects. Carriers would likely perform that inspection at the same time as a safety inspection.

Question 9.: What measures have been or can be implemented that serves both purposes of safety and security?

Mr. Rosapep: FRA considers security concerns when developing rail safety rules. For example, FRA's January 2002 final rule barring most extraterritorial dispatching of U.S. railroad operations addresses the agency's concerns about the security of foreign dispatching facilities. *See* 49 CFR Part 241. Similarly, in 1998 FRA issued a regulation requiring passenger railroads to prepare, and obtain FRA approval of, plans to address emergencies arising from accidental or criminal events, including security threats. Each plan must address employee training and qualification, provide for initial and recurrent training of employees on the plans and coordination with emergency responders, and provide for the conducting of emergency simulation drills with actual equipment and simulated victims. *See* 49 CFR Part 239. In addition, FRA's safety regulations can affect both safety and security. For example, FRA issued comprehensive safety standards for passenger equipment in 1999, including requirements for crashworthiness, fire safety, and emergency systems that help protect against, or reduce the consequences of, accidental events as well as deliberate acts. *See* 49 CFR Part 238. FRA will continue monitoring passenger railroads for compliance with this regulation and attend each full-scale simulation and follow-up review session, and has invited TSA to participate in these audits.

FRA has a passenger equipment rulemaking well underway that will help promote passenger and employee safety in an emergency situation whether resulting from accidental or intentional acts. The rulemaking would address passenger/crew communication systems, provide for enhanced requirements for emergency window exits in passenger cars, and mandate that all passenger cars, including existing cars, have rescue windows for emergency responder access. *See* 71 FR 50276; August 24, 2006. A separate FRA regulatory proposal in development would enhance current requirements for passenger car emergency signage and lighting, and introduce new requirements for low-location exit path marking.

In addition, FRA enforces in the rail mode of transportation the Hazardous Materials Regulations, which are promulgated by PHMSA. These regulations include requirements that railroads and other transporters of hazardous material, as well as shippers, have and adhere to security plans and also train their employees involved in offering, accepting, or transporting hazardous material on both safety and security matters. In December 2006 PHMSA proposed enhancements to its security plans requirements that would require carriers to choose the safest, most secure route, for the movement of certain hazardous materials. In addition, both agencies are jointly engaged in a comprehensive review of design and operational factors that affect the safety of transportation of hazardous material by railroad tank car and are hard at work on a proposal for better tank car design standards.

Finally, FRA conducts and supports research, development, and demonstration projects related to rail safety and rail security through its Office of Research and Development, in cooperation with DHS. Both theoretical and applied research on a wide range of issues has led to impressive results and to tangible technology and process improvements.

Question 10.: Do you believe that the risk assessments conducted with Amtrak are sufficient to prevent a potential terrorist attack?

Mr. Rosapep: Complementing FRA and TSA efforts, Amtrak has instituted its own security plan and conducts security training. FRA assisted Amtrak in the updating of its security plan. Specifically, in coordination with Amtrak's Inspector General, FRA contracted with the RAND Corporation to conduct a systematic review and assessment of Amtrak's security posture, corporate strategic security planning, and programs focusing on the adequacy of preparedness for combating terrorist threats. FRA, in conjunction with the Amtrak Board and management, has established goals based on the RAND study and has developed a substantive action plan for Amtrak to enhance its strategic security planning and better synchronize its overall risk management with cost effective security investment decisions. FRA's security director is currently working with Amtrak in implementing the recommendations of the RAND study. So far, in carrying out the action plan, Amtrak has hired a Vice President for Risk Management, made management and organizational changes at the Amtrak police force, and conducted drills and exercises with Federal, state and local agencies to leverage interoperability and resources. In addition, Amtrak is developing a comprehensive corporate security plan and security investment plan.

Chris Kozub from the National Transit Institute (NTI) has testified before our Committee on training for mass transit employees. In his testimony, he stated that NTI and FTA's training had reached about 20% of the transit employee workforce, which is approximated to be about 300,000. As of today that number has increased to slightly higher than 30%. While reaching 90,000 employees—many of whom are employed by the larger, security critical, metropolitan systems of the country—is a noteworthy accomplishment, NTI is still below the halfway point and has a lot of work still to do.

Question 11.: What steps have been taken to reach the remaining 70%?

Mr. Rosapep: In collaboration with TSA, FTA has obligated funds for an additional 80 deliveries of the following security courses:

—Terrorist Activity Recognition and Response;
—National Incident Management System Training for Transit Employees;
—Strategic Counter Terrorism Training for Transit Managers; and
—Chem/Bio for Operations Control Center Personnel.

FTA has developed a Strategic Curriculum Development Process for the development and revision of all FTA-sponsored safety and security courses. This process is in line with the DHS G&T requirement for course approval. To date, FTA has three security courses successfully revised into the new format which received approval from DHS G&T as "approved" courses. This benefits the grant recipient transit agencies as they can apply for training grants to take the course. (This assists in the funding of overtime and backfilling of positions when employees are sent to the training.) This action should assist the transit agencies by removing a funding barrier, making it easier for them to send employees to the training.

Additionally, FTA is in the process of assessing the top 30 transit agencies and smaller and rural transit properties to determine what training courses they have provided to their employees as well as whom they are requiring to be trained within their agency. This needs assessment will allow FTA and its partners to better serve the transit industry with regard to transit security training and understanding what barriers transit agencies are facing with regard to the implementation of training programs.

Finally, FTA, in collaboration with the National Transit Institute, is developing a comprehensive safety and security training DVD that will be sent out the targeted transit agencies to provide them with updated information on course overviews, training schedules, and registration and contact information. This will provide a one-stop shopping approach to enhance the availability of the training information.

It is with the above actions that we anticipate closing the gap of untrained transit employees.

Question 12.: Which agency is responsible for ensuring that all employees receive training?

Mr. Rosapep: Transit security training is a shared responsibility among FTA, TSA, and G&T. TSA and G&T have the ability to provide monetary resources that

will allow the transit industry to take advantage of existing training courses. FTA has the historical knowledge and established relationships with experienced training providers.

Question 13.: It is my understanding that as drafted the Notices of Proposed Rulemaking (NPRMs) recently released by TSA and the Department of Transportation will preclude state and local officials from mandating the rerouting of hazardous materials. Why did you include this provision in your NPRM?

Mr. Rosapep: State and local officials are already precluded from mandating the rerouting of hazardous materials under statutory preemption provisions at 49 U.S.C. §§ 20106 and 5125 (Sections 20106 and 5125). Section 20106 was originally enacted in the Federal Railroad Safety Act of 1970, then reenacted as positive law in the 1994 recodification, and subsequently amended; it requires that standards related to railroad safety and standards related to railroad security be "nationally uniform to the extent practicable." Under Section 20106, a State may adopt or continue in force a law, regulation, or order related to railroad safety or security until the Secretary of Transportation (with respect to rail safety matters) or the Secretary of Homeland Security (with respect to rail security matters) issues a regulation or order covering the subject matter of the State requirement.

PHMSA has covered the subject matter of rail routing of hazardous materials when it promulgated a final rule in 2003 that permitted railroads to tailor their en route security measures to their individual circumstance through required security plans. 49 C.F.R. § 172.800 *et seq.* See the Court of Appeals' decision in *CSX Transp., Inc. v. Williams,* 406 F.3d 667 (D.C. Cir. 2005). That decision also found that the exception in Section 20106 (which allows a State to have an additional or more stringent law, regulation, or order when the State law, regulation, or order (1) is necessary to eliminate or reduce an essentially local safety or security hazard, (2) is not incompatible with a Federal law, regulation, or order, and (3) does not unreasonably burden interstate commerce) is not applicable to the forced rerouting of rail shipments of hazardous materials.

PHMSA's December 21, 2006 proposed rule would add additional railroad security planning requirements with respect to routing of certain hazardous materials that will enhance the safety and security of the rail movement of these commodities. Railroads would be required to compile annual data on specified shipments of hazardous materials, use the data to analyze safety and security risks along rail transportation routes where those materials are transported, assess alternative routing options, and choose the routes that posed the least safety and security risk. The NPRM also contains provisions requiring DOT access to data, route analysis, and route selection. This would provide DOT with basic oversight of, and insight into, route analysis performed by carriers. If the chosen route is found not to be the safest and most secure, commercially practical route, FRA would be permitted to require use of an alternative route until such time as the identified deficiencies are satisfactorily addressed. The coordinated NPRM issued by TSA would also add chain-of-custody, attendance, and tracking requirements for rail cars containing these hazardous materials.

In addition, Section 5125 in the Federal hazardous material transportation law provides that a requirement established by a State, locality, or Indian tribe is preempted if it is not possible to comply with that requirement and a Federal requirement or compliance with the non-Federal requirement would create an obstacle to accomplishing and carrying out the Federal hazardous material transportation law or a regulation issued under that law.

Unlike truck routing, with its web of interstate highways, toll roads, bypasses, and two-lane rural roads crisscrossing the country, within the rail system there are only a limited number of routing alternatives. Rail lines generally run through, rather than around, major metropolitan areas, and many hazardous material shipments originate in, and/or are destined for, locations in heavily populated areas. It would be totally impracticable to allow States and cities to mandate the rerouting of hazardous materials in order to shift the security risks associated with the transportation of hazardous materials to other jurisdictions.

FRED WEIDERHOLD RESPONSES TO HON. BENNIE G. THOMPSON QUESTIONS

Note:

The questions posed in the initial information request have been renumbered in accordance with a reasonable clustering of their overlapping nature. In turn, some of the questions that do not directly relate to the responsibilities of the Amtrak Office of Inspector General have been eschewed, in favor of a focus on areas where

my office has recent and valid experience and knowledge. To this end the text and numbering of the questions is re-ordered in each of the responses below.

Question 1. Your industry has continuously resisted mandatory security plans and vulnerability assessments, which will be required by this legislation. However, ports, the chemical industry, and the aviation industry all have to submit mandatory plans to DHS. Why do you feel that your industry should be excluded from this requirement?

Response: I disagree with this characterization of the railroad industry position. The industry undertook a forward-leaning approach following 911, with independently designed security plans, vulnerability assessments, and threat based alert-systems all deployed consistent with developed industry standards. We exercised self-help when the Department of Homeland Security (DHS) and the Transportation Security Administration (TSA) seemed focused on the aviation sector, sometimes to the apparent exclusion of surface transportation matters. At the same time, the attention we did receive from TSA was at times grudging, and the result of consistent attempts by us to integrate our ongoing efforts into what we sometimes viewed as a flawed federal government approach to protecting critical infrastructure. Principal among our concerns is the preparedness of TSA inspectors—and inspections—to deal with the special safety and infrastructure peculiarities of the rail environment. Collaborative discussion of rail security and infrastructure protection concepts, alongside an acknowledgment by government that the assessments we have undertaken have *standing* relative to any new requirements for baseline security reviews, is the first step to making the sector security progress we all hold as a shared objective.

Question 2.: According to the GAO, the FRA has been focusing its efforts to improve rail safety, addressing issues such as human error, inspections, and rail track failure. It seems that the industry views safety as a bigger, more pressing concern than the risk of terrorism.

(a) Is there a nexus between safety and security concerns? Where do these issues overlap and where do they diverge?

There is undoubtedly a nexus between safety preparations and appropriately addressing security concerns. Protection of passenger, personnel, and public safety is the highest priority of the rail operator. Consistent with this value, we have implemented safety protocols designed to protect both the traveling public, our passengers, employees—and persons who have only incidental contact with our rights of way and infrastructure. Many of these measures have been implemented consistent with our obligations under federal regulations. In addition we have endeavored to conform to the spirit of the RAILPAX (02) security directives promulgated by TSA. We remain concerned that any security rules must be based in rigorous risk assessments. It is critically important that whatever progress we make in terms of terrorism risk mitigation not come at the cost of reductions in hard-won improvements in safety and accident prevention. Reconciling federal critical infrastructure protection objectives with parallel societal interests in enhanced safety is appropriately a subject of Congressional deliberations with the Administration.

(b) What measures have been or can be implemented that serves both the purposes of safety and security?

Improvements in passenger flow management promise dividends in both the safety and security domains. Amtrak has undertaken efforts at at least one major station to rationalize passenger movements within the facility to enhance the ability to control access to sensitive areas. In turn, these measures help to ensure against inadvertent passenger entry into areas where potentially dangerous infrastructure and equipment are located.

Regular inventories of changes in critical infrastructure equipment—and critical system features—help to ensure that potentially vulnerable areas receive timely assessment and protection. As railroads attempt to leverage advances in computing and communications technologies to achieve greater efficiencies, it is particularly important that continuous oversight be maintained on the safety and security significance of particular systems and operating processes. My office focuses much of its security oversight activities in this problem area.

Question 3.: Do you believe that risk assessments conducted with Amtrak are sufficient to prevent a potential terrorist attack?

Assessments by themselves are unlikely to be sufficient to prevent a potential terrorist attack. Nonetheless, assessments are a critical part of the process of understanding—and thereby reducing—the terrorism risk exposure of railroad operations. This is why the methodologies used in risk assessments must be both rigorous and validated ? hopefully through empirical testing in as many representative railroad

environments as possible. Similarly, those undertaking such assessments must be knowledgeable about the railroad sector, and sensitive to the historical record or terrorist attacks on passenger and freight rail. With this sound basis for assessments, suggested remedial measures can themselves be evaluated for cost-effective application to varying rail conditions.

Question 4.: Given the open nature of passenger rail systems—multiple access points, large crowds of people, and no barriers—can anything be done to protect these systems?

While passenger rail systems are difficult to protect, there are things that can be done to manage the risk to rail operations and to passenger and worker security. Among the measures that Amtrak and commuter rail operators have taken are: assessments of vulnerability in critical facilities such as stations and infrastructure elements, surveillance and counter-surveillance operations designed to deter against terrorist exploitation of infrastructure weaknesses, alert-based modifications to passenger flow inside stations to present a different 'defensive posture' to potential attackers who are undertaking surveillance, and increased uses of technology to detect potentially hazardous materials wherever they might be introduced within the public transportation system. All of these measures are designed to *harden* the passenger rail environment. It remains the case, however, that any hardening or deterrent effects that are achieved are themselves only relative, and may be time-bound and only conditionally effective, given uncertainties on the evolution of the terror threat.

Question 5.: How have you determined the greatest risk of attack for your system? What is the greatest risk?

Risk exposure for passenger (and freight) rail environments is assessed against the available threat information and vulnerability exposure of a particular infrastructure setting. Rigorous and frequent evaluations provide the information necessary to identify critical infrastructure and key assets that are fundamental to maintaining continuity of operations—as well as public (passenger) and personnel security. Information on key assets and critical node vulnerabilities is sensitive, and is not appropriately discussed in an open setting. I would be happy to share our insights on these subjects in a more controlled information dissemination process.

6. What is your response to criticism that the industry cannot be trusted to police itself?

I would challenge those that hold this view, with the information I related in response to question 1. The Class 1 railroads have undertaken considerable self-help in establishing a basis for sector infrastructure protection that matches many of the measures taken elsewhere in the U.S. What has been lacking until relatively recently is an acknowledgment by federal policy makers that the sector has adopted many measures equivalent in effect to proposed risk mitigation mandates articulated—often at a very superficial level—by our industry critics. Assessments by themselves do not improve the terrorism risk mitigation capabilities of the sector. Similarly, inspections will not by themselves do much to add protective and risk mitigation capacity. Instead, a virtuous cycle of inspections and evaluations, deployment of protective measures and protocols, and an evaluation of measure efficacy *using rigorously validated metrics for risk management* must be established. Once this is achieved, management of terror threats to passenger (and freight) rail will be placed on a much firmer basis.

Question 7.: You've stated previously that a difficulty with improving your security posture is lack of security standards. You went on to say that the directives prepared by DHS in 2004 "are not necessarily the comprehensive basis for an effective rail passenger security strategy." In your opinion, what should DHS do to provide industry with a comprehensive strategy?

A first set of measures that DHS could undertake would be to reconcile continuous calls for measures to improve terrorism risk management in the rail sector with an acknowledgment of the measures that have already been taken since 2004 to achieve the same end. Put succinctly, continual calls for assessments do not adequately acknowledge the progress already achieved in evaluating the criticality of rail infrastructure and process control elements. Much of rail is readily aware of its vulnerability exposure, and has undertaken measures designed to reduce that exposure. Acknowledgment that these measures have been taken, and a requisite revision to national and sector-wide protective strategies articulated by DHS and TSA, would be a tremendous improvement over the current situation. Once acknowledged, the focus of strategy-design would shift from a top-down protective effort to a more incrementally "do-able" reconciliation strategy, that would seek to "knit to-

gether" the efforts of the Class 1 and other (smaller) railroads—with those of the transit and commuter rail sectors—into a mutually reinforcing process of sector improvements. The security standards-creation (and/or security regulatory) process would thus be based on emerging industry best practices, rather than upon imposed regulations which are non-validated against meaningful metrics for assessing their value for terrorism risk mitigation.

Question 8.: Is it your opinion that rail and mass transit stakeholders are appropriately involved as TSA moves forward with current and future security efforts, such as the recently issued proposed rule on rail?

The SCC–GCC process within which passenger rail is consulted on appropriate responses to security/terrorism risk exposure, is one that has the potential to fully address sector concerns with respect to establishing an effective security regulatory framework. These efforts are a work in progress, and the establishment of working relationships between government agencies and railroad organizations is something that requires time and effort on both sides. I am cautiously optimistic that, with a genuine effort by all involved parties, concrete improvements in this area will be achieved.

Question 9.: TSA has recently issues a Notice of Proposed Rule making (NPRM) that would impose several new security requirements for rail carriers, rail transit systems; and rail operations at certain facilities that ship or receive hazardous materials. As part of this proposal, TSA would require rail and transit operators (as well as hazmat facilities) to allow physical inspection of their operations. In addition, chain of custody and hazmat tracking requirements will need to be enforced. **How many additional inspectors—TSA inspectors—do you anticipate will be needed for this expanded role?**

The answer to this question depends on the duties and training of the inspection force, together with developments in the "ambient" threat environment—against which the validity of protective measures must be continually evaluated. I am uncomfortable focusing on the number of inspectors as an appropriate index of the inspection capabilities necessary to maintain appropriate oversight of security developments (and regulatory compliance). Rather, emphasis should be placed on the empirical rigor and validity of the assessment methodologies used by these inspectors, and on the important differences that exist within different rail (passenger and freight), and industry settings. The TSA NPRM makes a number of assumptions relative to the likely development of autonomous security and best practice developments that might occur in industry *in the absence of government regulations.* These assumptions should be evaluated against the record since 2004 of industry leadership in the design and implementation of terrorism risk mitigation measures. The activities of inspectors—and the qualifications that these individuals should have before they are allowed on a rail property—should be determined in the context of developing industry best practices.

Question 10.: How would you compare the risks facing the passenger rail systems with the risks faced by other modes of transportation? Is the current allocation of federal resources for rail security commensurate with the unique risks these systems face?

Comparisons of terrorism risk exposure across critical sectors are inherently difficult. Achieving such a comparison among different transportation modes is doubly difficult and uncertain. After all, what criteria is one to use for assessing "relative" risk? History? Known vulnerability exposure? The "Revealed Preferences" of terrorists-as discerned through intelligence or informed opinion? It is perhaps safest to focus on the groups determined to pose the greatest threat to US homeland and national security, and then derive a relatively rigorous "threat profile" of their 'modus operandi' relative to infrastructure attacks—determining their favored targets, attack methods, and pre-attack surveillance behavior. Using such a methodology, it is difficult to avoid the conclusion that passenger rail is a favored target of terrorists—the terrorists with which we are most concerned—Al Qaeda and its jihadist adherents around the world. Events since 911 reinforce this conclusion, with Moscow, Madrid, London and Mumbai offering empirical validation of the frequency of attacks using explosives against passenger rail targets.

The critical question is: given this history, and revealed preference set of terrorists, are we doing all that can be done to increase the detection, deterrence and risk mitigation of potential attacks? Federal priorities should reflect the historical record of attacks against critical infrastructures—but they must also be sensitive to changes in the attack environment. Leveraging intelligence insights with a representative set of expert input might be the best way to appropriately capture the

dynamism of the risk environment—enhancing response sensitivity to the changing validity of selected response measures.

Question 11.: Is the President's budget request reasonable to help secure the Nation's rail and mass transit systems? Is the disproportionately low amount of TSA's budget ($41.4 million out of $6.4 billion) dedicated to rail and mass transit security and indication to your organizations that it is not a priority of DHS?

Historically, passenger rail has not received the security funding from the Federal Government commensurate with the apparent terrorism risks to which it is exposed. In turn, the grant mechanism for providing support has itself been changeable, typically favoring state and locally supported entities. Amtrak was not even eligible for security grants before FY2005. In the light of this funding and assessment environment, it can be observed that the low level of funding has been inconsistent with the recent history of attacks on passenger rail. At the same time, the threat environment is uncertain, and the exact level and nature of funding required to meaningfully improve terrorism risk management remains to be determined.

Question 12.: What are your thoughts in the utilization of security practices used by other countries?

As I noted in my responses to some of the other questions, the international experience with terrorist attacks on passenger rail is unfortunately rich with events and casualties. Different countries have varying experience in responding to these events, typically conditioned by their national legal systems, and historical experiences with terrorism.

It is undoubtedly the case that foreign countries have potentially usable experiences dealing with terrorism related to rail targets. Sensitive insights and information on rail-targeted terrorism is shared between law enforcement agencies in different countries. Much of this sharing takes place through established channels—structured agency to agency relationships crafted for other reasons. In the aftermath of the Madrid bombings my office facilitated links between the Guardia Civil in Spain and the Amtrak Police Department (and other interested stake holders)—whereby highly sensitive and otherwise unavailable insights were gained into the attack planning, device design, and operational practices—of a terrorist cell. After the Mumbai bombings insights were gained into device design and placement from specialists employed by the NYPD. These agents were deployed to India prior to those events, and were able to provide invaluable information on the nature of the attacks, and early investigative clues. Subsequently my office was able to use established contacts with Indian Railroad Ministry to gain even more insight into the lessons learned from that unfortunate incident.

The investigative and forensic analysis excellence of the British railroad police is widely acknowledged. Of special importance in the British context is the extensive use of railroad surveillance (i.e. CCTV) in reconstruction of the rail bombers plans and pre-attack practice. Also of note in the British context was the speed with which the rail system returned to normal operation following the attacks. This return to normal service was facilitated by the ability of responding agencies to instill confidence in the traveling public that they understood the nature of the terrorism risk confronting the rail system, and that they had taken appropriate near-term measures to manage that risk—enabling a return to something approximating normal service.

It is remains unclear the exact scope of the applicability of foreign experience to the U.S. Context. Public tolerance of wide-area surveillance of rail travel, and the use of operational modifications to rail travel habits as a risk mitigation measure, are largely untried in this country. Experimentation on different response regimes may allow for sustained progress in terrorism risk mitigation without compromising the advantages of the open and flexible rail environment. Federal policy should seek to foster the adoption of a varied set of protective responses—as both a means of increasing the protective efficacy of risk mitigation, but also to indicate to the public the continual prevalence of protection throughout all aspects of the U.S. Transportation system. Such an effort could help to allay perceptions that surface transportation modes receive less aggressive protection than is true of the aviation sector.