THE LONDON BOMBINGS: PROTECTING CIVILIAN TARGETS FROM TERRORIST ATTACKS PART I AND II

HEARING

BEFORE THE

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

SEPTEMBER 7, 2005 and OCTOBER 20, 2005

Serial No. 109–39

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

28–921 PDF WASHINGTON : 2007

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

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
PETER T. KING, New York
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL MCCAUL, Texas
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
BENNIE G. THOMPSON, Mississippi
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
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY

DANIEL E. LUNGREN, California, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
PETER T. KING, New York *(Ex Officio)*
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
PETER A. DEFAZIO, Oregon
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
JAMES R. LANGEVIN, Rhode Island
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

CONTENTS

Page

STATEMENTS

The Honorable Daniel E. Lungren, a Representative in Congress From the State of California, and Chairman, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity:
Oral Statement 11
Prepared Opening Statement, September 7, 2007 3
Prepared Statement, October 20, 2007 55
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security 4
The Honorable Norman D. Dicks, a Representative in Congress From the State of Washington 39
The Honorable James R. Langevin, a Representative in Congress From the State of Rhode Island 40
The Honorable Sheila Jackson-Lee, a Representative in Congress From the State of Texas 44
The Honorable John Linder, a Representative in Congress From the State of Georgia 38
The Honorable Bill Pascrell, Jr., a Representative in Congress From the State of New Jersey 35
The Honorable Stevan Pearce, a Representative in Congress From the State of New Mexico 74
The Honorable Mark E. Souder, a Representative in Congress From the State of Indiana 45

WITNESSES

WEDNESDAY, SEPTEMBER 7, 2005

Mr. Peter Lowy, CEO, Westfield America, Inc:
Oral Statement 11
Prepared Statement 13
Mr. Joe Madsen, Director, Safety and Risk Management, Spokane Public Schools, Spokane, Washington:
Oral Statement 25
Prepared Statement 27
Mr. Bill Millar, President, American Public Transportation Association:
Oral Statement 5
Prepared Statement 7
Mr. Michael Norton, Managing Director of Global Property Management, Tishman Speyer Properties:
Oral Statement 15
Prepared Statement 18

THURSDAY, OCTOBER 20, 2005

Mr. Robert Jamison, Deputy Administrator, Transportation Security Administration, Department of Homeland Security:
Oral Statement 64
Prepared Statement 66

Page

Mr. Robert Stephan, Assistant Secretary, Infrastructure Protection Division, Department of Homeland Security:
Oral Statement 57
Prepared statement 58

FOR THE RECORD

The International Council of Shopping Centers:
Prepared Statement, September 7, 2005 43
The Honorable Kip Hawley, Assistant Secretary, Transportation Security Administration, Department of Homeland Security:
Prepared Statement, September 7, 2005 87
Letter From Mr. Robert B. Stephan 93

THE LONDON BOMBINGS: PROTECTING CIVILIAN TARGETS FROM TERRORIST ATTACKS

Wednesday, September 7, 2005

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON ECONOMIC SECURITY,
INFRASTRUCTURE PROTECTION, AND CYBERSECURITY,
Washington, DC.

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

Present: Representatives Lungren, Linder, Souder, Thompson, Dicks, DeFazio, Lofgren, Jackson-Lee, Pascrell, and Langevin.

Mr. LUNGREN. [Presiding.] Good morning. I would like to welcome everyone to this hearing of the Committee on Homeland Security, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity.

We are meeting today for the first time in the committee's permanent hearing room, so maybe we will also get an office next to it at some time in the future, but we will work on that.

This morning, the subcommittee will focus on the protection of civilian or soft targets against terrorist attacks. A soft target can be any place or thing whose destruction or impairment will cause a loss of life, economic damage or psychological trauma, which is difficult to protect or harden because it is a location that is accessible to the public.

Soft targets would include schools, buses, trains, hotels, office buildings, restaurants, night clubs, apartment buildings, churches, mosques, synagogues or any place where many people can be found in close proximity.

It is true that in a free and open society such as ours, there are an infinite number of such potential targets which a terrorist could choose to attack. Compounding our difficulties, terrorists have many advantages. They have the ability to choose what, where, when and how to execute an attack. As the President has said, we have to be right 100 percent of the time, while they only have to get lucky once.

The latest tragedies in London and Egypt have highlighted the ease in which terrorists can perpetrate heinous crimes against the civilian population, even where reasonable security measures had already been instituted. Public transportation, particularly trains and buses, this has been the favored target of many high-profile at-

tacks, but terrorists have also repeatedly targeted night clubs, restaurants and hotels.

The inability to effectively restrict access and the potential for numerous casualties, combined with the psychological impact on the public and its resulting affect on our national economy makes these soft targets highly attractive to terrorists.

According to the RAND Memorial Institute for Prevention of Terrorism database of terrorist events, there have been almost 10,000 terrorist incidents worldwide since 9/11, of which more than 5,500 could be considered to have taken place against soft targets.

Increasing physical security of such sites is, of course, part of the solution to the challenge, but let's face it: screening every person accessing every possible soft target is both a physical and economic impossibility. Even if it were possible, there is simply no way to be 100 percent effective against a determined terrorist that is willing to take his or her own life in pursuit of the mission.

So accordingly, we must prioritize our efforts based on known risks and consequences, and avoid the temptation to focus on one soft target sector to the detriment of others. As Secretary Chertoff has said, terrorists are quite adaptable, so as we harden some types of facilities they would naturally switch to others that are seemingly less protected.

We must also figure out how to remain one step ahead of the terrorists and stop them before they execute their plans. We can accomplish this in large part by continuing to aggressively pursue intelligence regarding terrorists and their intentions.

And we can expand our intelligence-gathering capabilities further by training employees and civilians around or within soft targets to be watchful of suspicious behavior and attempt to intercept terrorists in the planning or reconnaissance or even implementation stages of an attack. Mass transit facilities and other security forces have begun doing this type of training already.

So I would like to welcome our witnesses today and thank them for participating in this timely discussion.

We had planned to have an initial panel with two witnesses representing the views of the Department of Homeland Security, the Honorable Kip Hawley, the Administrator of the Transportation Security Administration, and Robert Stephan, the Acting Under Secretary for Information Analysis and Infrastructure Protection. But given the need of these witnesses to be focused on the continuing response to Hurricane Katrina, we have decided to postpone that panel to another date later this month.

So our planned second panel now will be our only panel today. The witnesses represent a wide array of soft-target sectors, including mass transit, shopping malls, office buildings, and public schools. Let me restate that. Our witnesses represent a wide array of our economy, which, because of the nature of terrorism, makes them soft-target opportunities. As I say, they include mass transit, shopping malls, office buildings, and public schools.

The witnesses will provide us with important insights on the steps they have taken thus far to address the challenges posed by terrorists, the assistance they receive from DHS and other federal agencies, and what they believe the proper role of the federal government should be with respect to security within their sectors.

As I have said many times, we do not have all the wisdom in government and we can be well educated as to what is being done in the private sector. We would particularly like to concentrate on the cooperative nature of efforts between the private and public sector.

So I would like to thank the witnesses for appearing before us today and tell you that I look forward to your testimony.

I would recognize the Ranking Member of the full Committee, Mr. Thompson, who has been busy in the last week or so with some concerns in his own district as a result of the hurricane.

As you know, you have our best wishes and our prayers for the people in your district and the evacuees who have come to your district.

PREPARED OPENING STATEMENT OF HON. DANIEL LUNGREN

WEDNESDAY, SEPTEMBER 7, 2005

I would like to welcome everyone to this hearing of the Committee on Homeland Security Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity.

This morning, the Subcommittee will focus on the protection of civilian or "soft" targets against terrorist attacks.

A soft target can be any place or thing whose destruction or impairment will cause loss of life, economic damage, or psychological trauma, and which is difficult to protect or "harden" because it is a location that is accessible to the public.

Soft targets include schools, buses, trains, hotels, office buildings, restaurants, nightclubs, apartment buildings, churches, mosques, synagogues, or any place where many people can be found in close proximity.

In a free and open society such as ours, there are an infinite number of such potential targets from which a terrorist could chose to attack.

Compounding our difficulties, terrorists have many advantages—having the ability to chose what, where, when, and how to execute an attack. As the President has said, we have to be right 100 percent of the time, while the terrorists only have to get lucky once.

The latest tragedies in London and Egypt have highlighted the ease in which terrorists can perpetrate heinous crimes against the civilian population, even where reasonable security measures had already been instituted.

Public transportation—particularly trains and buses—has been the favored target in many high-profile attacks. But terrorists also have repeatedly targeted night clubs, restaurants, and hotels. The inability to effectively restrict access and the potential for numerous casualties—combined with the psychological impact on the public and its resulting effect on the national economy—makes these soft targets highly attractive to terrorists.

According to the RAND-Memorial Institute for Prevention of Terrorism database of terrorist events, there have been almost 10,000 terrorist incidents worldwide since September 11, 2001, of which more than 5,500 could be considered to have taken place against soft targets.

Increasing physical security at such sites is, of course, part of the solution to this challenge, but screening every person accessing every possible soft target is both a physical and economic impossibility. Even if it were possible, there is simply no way to be 100% effective against a determined terrorist that is willing to take his or her own life in pursuit of the mission.

Accordingly, we must prioritize our efforts based on known risks and consequences, and avoid the temptation to focus on one soft target sector to the detriment of others. As Secretary Chertoff has said, terrorists are quite adaptable, so as we harden some types of facilities, they will switch to others that are less protected.

We also must figure out how to remain one step ahead of the terrorists and stop them before they execute their plans. We can accomplish a large part of this by continuing to aggressively pursue intelligence regarding terrorists and their intentions.

And we can expand our intelligence gathering capabilities further, by training employees and civilians around or within soft targets to be watchful of suspicious behavior—in an attempt to intercept terrorists in the planning, reconnaissance, or

even implementation stages of an attack. Mass transit facilities and other security forces have begun doing this type of training already.

I'd like to welcome our witnesses today and thank them again for participating in this timely discussion.

We had planned to have an initial panel with two witnesses representing the views of the Department of Homeland Security: the Honorable Kip Hawley, Administrator, Transportation Security Administration, and Robert Stephan, Acting Under Secretary for Information Analysis and Infrastructure Protection. But given the need for these witnesses to be focused on the continuing response to Hurricane Katrina, we have decided to postpone this panel to another date later this month.

So our planned second panel will now be our only panel today. The witnesses represent a wide array of soft target sectors, including mass transit, shopping malls, office buildings, and public schools. These witnesses will provide us with important insights on the steps they have taken thus far to address the challenges posed by terrorists, the assistance they have received from DHS and other Federal agencies, and what they believe the proper role of the Federal government should be with respect to security within their sectors.

I would like to thank the witnesses for appearing before us today and I look forward to your testimony.

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

Let me acknowledge Mr. Pascrell and a number of other members of the committee who also called during what has been and continues to be a very trying time for this entire country, and more specifically for the people of Louisiana, Alabama and Mississippi.

But as you know, the matter we have before us today is a very important issue for this country. Like all Americans, I was shocked and repulsed by the terrorist attacks in London. This latest attack should serve as a reminder that America and its close allies continue to face a determined enemy that thinks nothing of slaughtering innocent people.

Now, after seeing the numerous failures to adequately prepare and respond to the Hurricane Katrina situation, I have my doubts about our nation's plans for dealing with emergencies. If we cannot handle a hurricane that we know is coming 4 days before, how can we trust that we are prepared for a catastrophic terrorist attack that we do not know about?

Because we live in an open and democratic society, we are particularly vulnerable to terrorists who live among us. This is especially true when it comes to our mass transit systems. Our mass transit and rail systems are large, open systems carrying billions of passengers a year, making it a prime target for terrorists.

Almost 4 years after the September 11 terrorist attack, passenger, rail and transit security remains a Department of Homeland Security afterthought. While the United States spent $11 billion on aviation security since 9/11, we managed to offer up $450 million for transit security. That is simply too little and too short, especially when one considers that Americans take mass transit 16 times more often than they travel by air.

This disparity, frankly, sends chills down my spine when I consider the pattern of train bombings overseas, first in Madrid, then in Moscow, and most recently in London. If the recent past is any guide, what is to prevent New York, Washington or Chicago from being next?

With the establishment of the Department of Homeland Security, the American people expected the department to help prevent such attacks. I would have to like to hear from the department who is

doing this, but in the instance of this catastrophe we are dealing with, we will deal with it later.

What I would like for them to do when they do come, Mr. Chairman, is provide us with the transit security plan that was due April 1 of this year. I have sent two letters to the administration indicating that you are overdue with this transit security plan, but I have yet to receive a response to those letters. It is sort of indicative of why we are behind right now.

Trains are not the only targets of al-Qa'ida and like-minded groups, as terrorists have attacked hotels in Saudi Arabia, a night club in Indonesia, and worst of all, a school full of children in Russia.

I would like to hear from the witnesses today what measures are in place to protect these soft targets and what has DHS done to address it. We will look at it when they come.

Mr. Chairman, I really would like to know whether or not in emergencies like we had with Katrina how our mass transit systems could potentially have helped with the evacuation of people, especially in the New Orleans area.

And after that, how soon could we get our system up and running? In London, they did it in a day after the bombings. I wonder what it would take us, with any kind of event, to get our systems up and running again? Since we are supposed to have a plan, I would like to hear it.

I look forward to the witnesses' testimony, and I yield back.

Mr. LUNGREN. I thank the Ranking Member, Mr. Thompson.

Other members of the Committee are reminded that opening statements may be submitted for the record.

We are pleased to have one distinguished panel of witnesses before us today on this important topic. As I mentioned, Assistant Secretary Stephan has been and continues to be working more than 18 hours a day at the command center dealing with the Katrina devastation. Assistant Secretary Hawley is also working on the Katrina response. The Subcommittee plans on having both of them in later this month to answer questions on this critical issue.

Let me remind the witnesses that your entire written statement will appear in the record. Because of the number that we have and the number of members we expect to be asking questions, we would ask that in accordance with committee rules you would limit your oral testimony to approximately 5 minutes, and then we would allow each panel member to testify before questioning any one of the witnesses.

The chair would first recognize Mr. Bill Millar, President of the American Public Transportation Association.

Mr. Millar, thank you for being here.

STATEMENT OF BILL MILLAR

Mr. MILLAR. Thank you, Mr. Chairman and members of the committee. On behalf of the 1,500 members of the American Public Transportation Association, we are certainly glad to be here.

It is very clear from your opening statement and Mr. Thompson's opening statement that the committee already has a very good understanding of some of the potential that public transit has to be

a target and some of the funding disparities, in our opinion, that have occurred over the years.

Quite simply put, we need to invest more money. We need to have better intelligence, and we need to do a better job of planning both for prevention and recovery. Those would be the three fundamental points of my testimony.

In light also that we find ourselves the week after Katrina, it is also important to realize that much of the investment in making our transit systems more secure can also assist in meeting national and natural disasters such as Katrina represents. I will be pleased to make further comments upon that point during the question period.

Public transit in America is a major form of public transportation. Every year, over 9.6 billion customers use public transit. Every weekday, 32 million times every weekday, Americans use public transit. And as has been pointed out, this is 16 times the number of people who use our nation's airline system, and yet the expenditure by the federal government to make public transit more secure is minuscule compared to the federal investment in the air system. We all understood and understand why the air system needs to be made secure, but now it is time to look at other parts of our transportation system.

As you pointed out, Mr. Chairman, over the last 25 years public transit around the world has too often been a target of terrorist attack. While we are focused on the most recent events such as London or Madrid or Moscow, the list goes on and on and on. Thus, prior to 9/11/2001, our industry knew that we could be a target. Our industry had already in place many plans and had taken many steps to try to improve its dealing with security issues. However, much more needs to be done.

Since 9/11, the industry has invested out of its own resources more than $2 billion in improving our security and preparing for terrorist attacks and in developing plans for recovery in the even that, God forbid, such an attack would occur in the United States. We do not need more wake-up calls. We need help. We need plans for action. We need investment.

We did a survey of our members which we released about 1 1/2 years ago asking that, at that point, we were 2 years into the post–9/11 environment. We knew that more needed to be done. What did our members tell us out of that survey?

They told us several things. First, I have already referred to the $2 billion that at that point they had invested themselves. Second, they felt that a major capital investment approaching $5.2 billion was necessary to take common sense solutions.

You are quite right, Mr. Chairman. None of us believe that you could totally insulate public transit systems from the potential of terrorist attack, but we do believe that there are many common sense steps that could be taken, such things as improving preparedness planning, training, drilling; such things as improving the communications systems of our transit systems; improving the access points to our access systems; and many, many common sense steps that could be taken.

Regrettably, sufficient funds have not been provided to undertake these steps. This current fiscal year, the Congress appro-

priated $150 million to cover all of public transit, passenger, freight and rail security. That simply is not a large enough investment. More needs to be done.

According to our survey, what did we find? Well, we find that over 2,000 rail stations in America do not have any security cameras. Some additional work we did subsequent to that revealed that 53,000 buses do not have cameras on those buses. Over 5,000 commuter rail cars do not have security cameras. Over half of all buses do not have automatic vehicle locator systems. And the list goes on and on and on.

Certainly, we saw something in New Orleans that ought to make us all think about this next statistic. More than 75 percent of the demand-response vehicles, the small vehicles that are used primarily to transport persons with disabilities or senior citizens or others in that type of need, over 75 percent of those vehicles lack automatic vehicle locator systems.

There is no permanent biological detection system in any rail transit system in America.

And the list goes on and on and on.

The second area I mentioned relates to the need for intelligence. After 9/11, in cooperation with the Federal Transit Administration, a federal public transportation-funded ISAC program, Information Security Analysis Center, was set up throughout the country. Regrettably, the funding for that ISAC center and the great intelligence that it provided to transit systems across the country has expired.

The Department of Homeland Security has offered a substitute, allowing us to tap into what they call their Homeland Security Information Network, the HSIN Network. However, in our judgment, this is no substitute for the ISAC that has already proven its worth and is already in place. So we certainly need to work on how we can get more information access to intelligence.

We need to make sure that when the terror alert level is raised that everyone understands that has major costs to that. For example, a survey we did this last summer showed that when the alert level was raised to orange, simply going up one step, even though nothing happened, we found that that added $900,000 a day to our costs. In the time between July 7 when the London bombings occurred and the threat level was raised, until August 12 when it was lowered, transit systems incurred over $33 million in costs.

So the list goes on and on. I am sure my time is about done. I will be happy to expand on these or any other points as may be appropriate.

Thank you, again, Mr. Chairman and members of the committee, for your concern and allowing me to be with you.

[The statement of Mr. Millar follows:]

PREPARED STATEMENT OF WILLIAM W. MILLAR

WEDNESDAY, SEPTEMBER 7, 2005

Mr. Chairman, thank you for this opportunity to testify on the security and safety of public transportation systems. We appreciate your interest in transportation security, and we look forward to working with you on these issues.

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 our nation's critical infrastructures. We cannot over-emphasize the critical importance of our industry to the economic quality of life of this country. Over 9.6 billion transit trips are taken annually on all modes of transit service. People use public transportation vehicles over 32 million times each weekday. This is more than sixteen times the number of daily travelers on the nation's airlines.

Safety and security are the top priority of the public transportation industry. Transit systems took many steps to improve security prior to 9/11 and have significantly increased efforts since then. Since September 11, 2001, public transit agencies in the United States have spent over $2 billion on security and emergency preparedness programs and technology from their own budgets with only minimal federal funding. This year's events in London and last year's events in Madrid further highlight the need to strengthen security on public transit systems and to do so without delay. We do not need another wakeup call like London and Madrid.

In 2004 APTA surveyed its U.S. transit system members to determine what actions they needed to take to improve security for their customers, employees and facilities. In response to the survey, transit agencies around the country have identified in excess of $6 billion in transit security investment needs. State and local governments and transit agencies are doing what they can to improve security, but it is important that the federal government be a full partner in the effort to ensure the security of the nation's transit users.

In FY 2003, transit security was allocated $65 million in federal funds for 20 transit systems from DHS. In FY 2004, $50 million was allocated for 30 transit systems from DHS. For the first time in FY 2005, Congress specifically appropriated $150 million for transit, passenger and freight rail security. Out of the $150 million, transit is to receive approximately $130 million—almost $108 million for rail transit and more than $22 million for bus. Also, passenger ferries are slated to receive an additional $5 million for security from a separate account. We are very appreciative of this effort. However, in the face of significant needs, more needs to be done.

We urge Congress to act decisively on this issue. In light of the documented needs, we have respectfully urged Congress to provide $2 billion in the FY 2006 Homeland Security Appropriations bill for transit security. Of that amount, we recommended that $1.2 billion be provided for capital needs, and $800 million for additional transit security costs. Federal funding for additional security needs should provide for, among other things, planning, public awareness, training and additional transit police.

Transit authorities have significant and specific transit security needs. Based on APTA's 2003 Infrastructure Database survey, over 2,000 rail stations do not have 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 do not have security cameras. Less than one-half of all buses have automatic vehicle locator systems (AVL's) that allow dispatchers to know the location of the bus when an emergency occurs. Nearly 75% of demand response vehicles lack these AVL's. Furthermore, no transit system has a permanent biological detection system. In addition, only two transit authorities have a permanent chemical detection system. A partnership with the federal government could help to better address many of these specific needs.

We were disappointed that the Administration recommended only $600 million for a Targeted Infrastructure Protection Program in the FY 2006 DHS budget proposal, which would fund infrastructure security grants for transit, seaports, railways and energy facilities. We were also disappointed that the Administration did not include a specific line item funding amount for transit security. We look forward to working with the Administration and Congress in securing adequate transit security funding that begins to address unmet transit security needs throughout the country.

We further request that the existing process for distributing DHS federal grant funding be modified so that funds are distributed directly to transit authorities, rather than to State Administrating Agencies (SAA). While we understand the need to coordinate with the states and urban areas that we serve, we believe direct fund-

ing to the transit authorities would be more efficient and productive. For the FY2003 grant funding that was allocated by DHS, it took more than a year to be awarded to some transit systems. In addition, the FY2005 grant funding has not been awarded to the transit systems to date.

We are pleased to note that APTA has become a "Standards Development Organization" (SDO) for the public transportation industry. Our efforts in standards development for commuter rail, rail transit and bus transit operations over recent years have been significant and our status as a SDO has been acknowledged by both the Federal Transit Administration (FTA) and the Federal Railroad Administration (FRA). The FTA and the Transportation Research Board have also supported our standards initiatives through the provision of grants. We would like to apply our growing expertise in standards development to transit industry safety and security, best practices, guidelines and standards. We look forward to working with the Administration and Congress in support of this initiative and trust that federal financial assistance would be made available to develop such standards and practices.

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.

INFORMATION SHARING

Since the terrorist attacks of September 11, 2001, public transit systems across the country have worked very hard to strengthen their security plans and procedures and have been very active in training personnel and conducting drills to test their capacity to respond to emergencies. As well, to the extent possible within their respective budgets, transit systems have been incrementally hardening their services through the introduction of additional technologies such as surveillance equipment, access control and intrusion detection systems. While the transit systems have been diligent, they have been unable to fully implement programs without more assistance from the federal government.

A vital component of ensuring public transit's ability to prepare and respond to critical events is the 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 "Information Sharing Analysis Center (ISAC)" for public transit systems throughout the United States. A funding grant in the amount of $1.2 million was provided to APTA by the Federal Transit Administration to establish a very successful Public Transit ISAC that operated 24 hours a day, 7 days a week, and gathered information from various sources, including DHS, and then passed information on to transit systems 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 then had to look for an alternate method of providing security intelligence through DHS's newly created "Homeland Security Information Network (HSIN)." APTA is now in the process of transitioning from the successful Public Transit ISAC to the new HSIN network. However, we believe that consistent, ongoing and reliable funds from Congress should be provided for the Public Transit ISAC that has been proven an effective delivery mechanism for security intelligence.

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

COST OF HEIGHTENED SECURITY

Following the attacks on London, APTA was asked to assist the 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 systems and extended periods pose significant impacts on personnel costs. These costs totaled $900,000 **per day** for US public transit systems 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 systems are also implementing other major programs to upgrade security. For example, New York's Metropolitan Transportation Authority 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 $212 million security upgrade announced late last month with the Lockheed Martin Corporation.

SECURITY INVESTMENT NEEDS

Mr. Chairman, since the awful events of 9/11, the transit industry has invested some $2 billion of its 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 latest 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.

Mr. Chairman, the Department of Homeland Security issued directives for the transit industry in May 2004, which would require that transit authorities beef up security and to take a series of precautions which would set the stage for more extensive measures without any federal funding assistance. Transit systems have already carried out many of the measures that Transportation Security Administration (TSA) is calling for, such as drafting security plans, removing trash bins and setting up procedures to deal with suspicious packages. The cost of these measures and further diligence taken during times of heightened alert is of particular concern to us. We look forward to working with you in addressing these issues.

As you know, in the FY 2005 Homeland Security Appropriations bill (PL 108–334), TSA can hire up to 100 rail inspectors using a $10 million appropriation. We have concerns about this provision. We believe that funding for the inspectors would be better spent on things that would support the industry such as surveillance cameras, and emergency communication and other systems rather than highlighting security issues without providing the necessary resources to address them. We look forward to working with you in addressing our concerns.

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. Shortly after the September 11 events, the APTA Executive Committee established a Security Task Force. The APTA Security Task Force has established a security strategic plan that prioritizes direction for our initiatives. Among those initiatives, the Task Force serves as the steering group for determining security projects with more than $2 million in Transit Cooperative Research funding through the Transportation Research Board.

Through this funding, APTA has conducted four transit security workshop forums around the nation for the larger transit systems with potentially greater risk exposure. These workshops provided confidential settings to enable sharing of security practices and applying methodologies to various scenarios. The outcomes from these workshops were made available in a controlled and confidential format to other transit agencies unable to attend the workshops. The workshops were held in New York, San Francisco, Atlanta, and Chicago.

In partnerships with the Transportation Research Board, the APTA Security Task Force has also established two TCRP Panels that identified and initiated specific projects developed to address *Preparedness/Detection/Response to Incidents* and *Prevention and Mitigation*. The Security Task Force emphasized the importance for the research projects to be operationally practical.

In addition to the TCRP funded efforts, a generic *Checklist For Transit Agency Review Of Emergency Response Planning And System Review* has been developed by APTA as a resource tool and is available on the APTA web site. Also through the direction of the Security Task Force, 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.

APTA has long-established Safety Audit Programs for Commuter Rail, Bus, and Rail Transit Operations. Within the scope of these programs are specific elements pertaining to *Emergency Response Planning and Training* as well as *Security Planning*. In keeping with our industry's increased emphasis on these areas, the APTA Safety Audit Programs have been modified to place added attention to these critical elements.

CONCLUSION

Mr. Chairman, in light of our nation's heightened security needs post 9/11, we believe that increased federal investment in public transportation security by Congress and DHS is critical. The public transportation industry has made great strides in transit security improvements since 9/11 but much more needs to be done. We look forward to building on our cooperative working relationship with the Department of Homeland Security and Congress to begin to address these needs. We again thank you and the Committee for allowing us to testify on these critical issues, and look forward to working with you on safety and security issues.

Mr. LUNGREN. Thank you very much, Mr. Millar, for your testimony.

The chair would now recognize Mr. Peter Lowy, the CEO of Westfield America, Inc., to testify.

Thank you for coming, sir.

STATEMENT OF PETER LOWY

Mr. LOWY. Thank you and good morning, Mr. Chairman. My name is Peter Lowy. I am the chief executive of the Westfield Group.

Westfield is, in terms of equity market capitalization, the world's largest publicly traded real estate company, with an equity market capitalization of over $23 billion. We own and operate 129 regional shopping malls in four countries: Australia, New Zealand, the United Kingdom, and here in the United States, where we own 68 regional shopping centers and manage the retail concessions at nine major airports, including terminals at JFK, Logan, Miami, Dulles and Reagan National.

I am testifying today on behalf of the Real Estate Roundtable.

In my written testimony, there are a number of broad suggestions with regard to business and homeland security relations that while I believe would be helpful, seem almost trivial in light of Hurricane Katrina. I would be happy to discuss those suggestions with the staff or the committee at a later date.

It is clear from the country's response to the devastation in Louisiana, Mississippi and Alabama that we are not adequately pre-

pared for the aftermath of a terrorist attack. Democracy and the political process that we are governed by, is by definition reactive.

The issues that business and government need to deal with fall into three interrelated categories. They are communication, coordination and preparedness.

From a communication point of view, things as simple as an organizational chart should be distributed so that we in business, and presumably the government, know who is responsible for what; whom to deal with for what issue; and most importantly, who is actually in charge.

At Westfield, our security plans assume the new normal is a yellow alert level. However, we do not know if our normal operating systems are consistent with what the government might consider appropriate for a yellow alert level.

Business often receives no indication of what threats we should be protecting against. And if they are identified, there is no standard for us to look at that tells us how to protect against that particular type of threat. A published list by Homeland Security of best practices, tied to specific types of threats, for example, would be extremely useful and helpful.

As you may know, Westfield owned the leasehold on the retail mall at the World Trade Center prior to 9/11. Because of our involvement in the World Trade Center, we unfortunately have direct knowledge of the issues that a terrorist attack can cause, whether they are personal, corporate, legal, economic, or insurance-related. From a coordination and preparedness point of view, prior to 9/11 Westfield implemented a nationwide program to improve coordination between ourselves and first responders. We also photographed all of our centers and fully digitized those photographs and the building plans, including those of the World Trade Center. The idea is to create a database that can effectively and efficiently be shared with first responders.

As you know, the Port Authority offices were destroyed on 9/11, and all of the paper building plans were destroyed with it. So the emergency personnel did not have the use of the blueprints for search and rescue operations. We realized immediately after the attack that we actually had the plans digitized. However, we literally could not find anyone to give them to. Finally, 10 days after 9/11, with the help of the mayor's office, we were able to get those plans to FEMA and the Office of Emergency Management to assist rescue and recovery workers in their efforts.

This experience resulted in our placing renewed emphasis on building solid lines of communication between ourselves, the local police, and fire and emergency departments at each of our locations. There is no doubt that 9/11 accelerated our security program and our investment in technology, people, systems, and increasing working relationships with our first responders. We sometimes even need to provide the technology that the local authorities need in order to access our information.

We have now built strong relationships between the local authorities and ourselves. We have held tabletop exercises in our Los Angeles headquarters with the LAPD, L.A. Fire Department, FBI, DHS, U.S Secret Service, Los Angeles Sheriff's Department and other local emergency responders. We also staged joint drills and

training exercises with those authorities in the many local jurisdictions where we have shopping centers across the country.

In summary, I think that the events of the past week have clearly demonstrated that Congress must aggressively pursue its oversight of the government's planning and execution for all activities related to homeland security.

Congress must work with DHS and all relevant state and local entities so that clear lines of communication exist for coordinated action to be carried out. The explosion of a biological or nuclear bomb or multiple conventional terrorist attacks in a major city can cause similar problems as those we have witnessed in New Orleans.

Congress must make the effort to see around the corner and designate with strict precision who is responsible for all major facets of the government's response to a terrorist attack, in order to best mitigate the potential damage and loss of life.

The private sector can work to take as many proactive measures as possible. As a mall owner, we can practice getting our customers and tenants safely out of the door. However, an effective evacuation will demand that the police can secure the routes, the city can provide potential medical relief if needed, and the state can provide transportation.

Congress must do all possible to achieve a comfort level that Homeland Security and all relevant government entities will work and communicate in the execution of these crucial plans.

I thank you for your time and would be happy to answer any questions after.

[The statement of Mr. Lowy follows:]

PREPARED STATEMENT OF PETER LOWY

WEDNESDAY, SEPTEMBER 7, 2005

Good morning Mr. Chairman and Members of the Committee. Thank you for this opportunity to address you this morning.

My name is Peter Lowy and I am the Chief Executive of The Westfield Group. By way of reference, Westfield is in terms of equity market capitalization the world's largest publicly-traded real estate company with an equity market capitalization of over $23 billion dollars. We own and operate 129 regional shopping malls in four countries—Australia, New Zealand, the UK and here in the US where we own 68 regional shopping centers and manage the retail concessions at 9 major airports including terminals at: JFK, Logan, Miami, Dulles and Reagan National.

I am testifying today on behalf of the Real Estate Roundtable.[1]

I think I am in a somewhat unique position to discuss this issue. As you may know, Westfield owned the leasehold on the retail mall at the World Trade Center prior to 9/11. Because of our involvement in the World Trade Center we unfortunately have direct knowledge of the issues that a terrorist attack can cause—whether they are personal, corporate, legal, economic or insurance related, as well as firsthand experience in trying to cope with the new reality that malls as public gathering places are considered to be targets for potential terrorist activity.

Because we view our malls as "town centers," even prior to the recent events in London and before 9/11, Westfield was looking for more effective ways to keep our centers—and thus our customers and employees—safe. For instance, we had begun a nationwide program to (1) improve communication and coordination between ourselves and first responders and (2) photograph our centers and fully digitize them

[1] The Real Estate Roundtable is the organization that brings together leaders of the nation's top public and privately-held real estate ownership, development, lending and management firms with the leaders of major national real estate trade associations to jointly address key national policy issues relating to real estate and the overall economy. The Roundtable provides day-to-day operational staffing of the Real Estate Information Sharing and Analysis Center.

and the building plans—including those of the World Trade Center. The idea is to create a database that can be efficiently shared with responding governmental entities so that first responders can know very quickly where all the points of entrance and egress are—how to access the roof, the HVAC and other sensitive areas. We did this because we took on the view that while we may not necessarily be able to stop a terrorist event—we have an obligation to try to mitigate the damage one might cause in terms of death, injury and property damage.

As you know, the Port Authority offices were destroyed on 9/11 and all of the paper building plans were destroyed with it—so that the City and first responders were lacking the blueprints of the structures. We realized immediately after the attack that we had the plans digitized—however, we literally couldn't find anyone to give them to. Finally, 10 days after 9/11 and with the help of the Mayor's office we were able to get the plans to FEMA and OEM to assist rescue and recovery workers in their efforts. This experience caused us to place renewed emphasis on building solid lines of communication between ourselves and local police, fire, and emergency departments.

There is no doubt that 9/11 accelerated our security program and we invest in technology, in people, in systems, in creating active working relationships with first responders—we sometimes even need to provide the technology that local authorities need in order to access and understand our information. In the US alone (since 9/11), 20% of our operating costs are now devoted to security, that's approximately $40 million per year, and 20–25% of our operating capital expenditures have been diverted to security infrastructure. But, as I have alluded to, arguably the most important—and most challenging—piece of this is the most low-tech of all. . .basic communication between the private sector and the local and federal authorities.

Firstly, I recognize as a business person that building strong relationships between local authorities and other key agencies is a priority. That is why we have held table top exercises in our Los Angeles headquarters with the LAPD, LA Fire Department, FBI, DHS, US Secret Service, Los Angles Sheriffs Department and other local emergency responders. We have also staged joint drills and training exercises with those authorities in the many local jurisdictions where we have shopping centers across the country. As an observer and a participant in this process, it has been my observation that one of the most difficult issues to solve is the lack of communication and coordination between ourselves, the local authorities and the FBI and the Department of Homeland Security. However, I understand that DHS has launched a new initiative in the form of placing in the field "Protective Security Advisors" to provide better coordination between Washington and the rest of the country. And there have been other outreach efforts including local Homeland Security Advisory Councils—which I have recently become involved in the greater-LA and Orange County region. These and other initiatives are important as the communication gap must be closed in order for prevention and response to be effective.

No where is this more telling than in the threat-level system. While again progress has been made, we all know of instances where the level has been elevated without business leaders then hearing from the government what measures we ought to take in order to meet that higher level of threat.

Our security plans assume that the new, "normal" is a yellow alert level. However, we don't know if our normal operating systems are consistent with what the government might consider appropriate for a yellow threat level. So that if there is an incident at one of our centers, I can almost guarantee that someone will sue us and make the argument that we didn't operate up to par with what a company should be doing under a yellow alert. However, business often receives no indication of what threats we should be protecting against. And if they are identified, there is no standard for us to look to that tells us how to protect against that particular type of threat. While I am not looking to codify some new set of lengthy government regulations, it would be helpful to create for business some "safe harbor" in the event of litigation after a terrorist incident. One way DHS might assist business would be to publish a list of "best practices" tied to specific types of threats and then encourage insurers to incentivize them.

I have here an internal document that shows how a mall such as ours might deal with the various threat levels. This is obviously a sensitive document that I would be hesitant to put into the official public record but I would be very happy to review it and share it with the Members of the Committee and the staff if that is helpful to them.

Currently, insurers have incentives in place for certain building improvements to better protect the property in case of earthquake, flooding and other natural disasters. In theory, if insurers are provided guidance from federal or local authorities as to best practices in security—they can then in turn incentivize their policy holders. I am working with other CEOs around the country as a Member of the Advisory

Board of Rand's Center for Terrorism Risk Management Policy where we are focusing on this issue of how insurance should function in the post 9/11 economy. Rand currently has a study that is underway which will look at the factors that affect the security decision-making of commercial real estate owners and will include insurance company incentives—or the lack thereof. I would be pleased to share the results of this research with the committee when they are available.

However, a recent Rand's study, "Trends in Terrorism" did touch on this subject. That report stated: "a long-run solution to terrorism should be designed to incorporate specific mechanisms, such as security-based premiums discounts, so that appropriate security investments can be encouraged through private insurance." Needless to say, in order for insurance to create incentives coverage needs to be available in the marketplace; so while I know its not the focus of this hearing I feel bound to remind you how important it is for Congress to extend the Terrorism Risk Insurance Act.

As part of their outreach to the private sector, I know that DHS has been working with industry groups and the Chamber to address the need for more specific guidelines to the color code system. Clearly, this is positive. I would simply urge that more communication with the business community—and especially businesses like ours which thrive on drawing large numbers of people to our properties—is necessary if we are to be truly prepared for an emergency situation.

The Rand "Trends in Terrorism" study has made it clear that the US Government's War on Terrorism has changed the operational environment of al-Qa'ida and other terrorist groups to softer targets that are easier to attack and more likely to be in the private sector. This trend has been exacerbated by target hardening around prominent sites—which has triggered a process of threat displacement to the easier to attack, civilian-frequented locations.

In summary, it is my opinion that at the heart of any cooperative efforts between the government and the private sector lays clear and reliable lines of communication. With more direction from DHS as to "best practices" and with insurers showing a willingness to reward policy holders for instituting them, I believe business would spend their limited resources more wisely and with greater benefit to the public. If we accept that soft targets have in fact become more attractive to terrorist cells, then it is especially important that a vibrant private-public partnership continue to develop and from that provide the business community with the best tools possible to secure our properties and most especially our employees and customers.

Mr. LUNGREN. Thank you very much, Mr. Lowy, for your testimony.

The chair would now recognize Mr. Michael Norton, Managing Director of Global Property Management for the Tishman Speyer Properties, to testify.

Thank you, sir, for coming.

STATEMENT OF MICHAEL NORTON

Mr. NORTON. Thank you, Mr. Chairman and members of the committee.

My name is Michael Norton. I am responsible for directing all property management activities at Tishman Speyer both in the U.S. and globally.

Our company is one of the leading owners, developers, fund managers and operators of first-class real estate in the world, with a property portfolio totaling more than 42 million square feet in major metropolitan areas across the United States, Europe and Latin America. Notably, our portfolio includes Rockefeller Center, the MetLife Building and the Chrysler Building in New York City.

I am testifying today on behalf of the Real Estate Roundtable, the Real Estate Board of New York, and BOMA International.

Thank you for holding what I believe is the first congressional hearing since the events of 9/11 at which major real estate companies and their associations have been invited to share their experience and expertise in security-related matters.

As a company and as an industry, we are committed to managing the risk of future acts of terrorism. That commitment is, of course, influenced by the expectations and demands of our various constituents including our tenant customers, our lenders, investors, insurers, legal advisers and local, state and federal government. In the end, any approach to security in buildings will need to be supported by all those constituents in order to be successful over the long term.

As an industry, we are spending over 20 percent more on security than we were pre–9/11. And yet, in the end, managing the risk of terrorism is not principally about spending more money. It is about strategically using existing resources to cost-effectively mitigate risks. Access to information, experience and best practices are assets that are hard to put a hard-dollar number on and yet they may be the most critical resources we have.

In my statement, I have detailed specifically some of the risk mitigation measures we have implemented at our company for the buildings I mentioned above and for other high-profile properties. These best practices fall into six basic categories: communications; emergency response, including emergency area access; training programs; hardening techniques; information sharing; and coordination initiatives.

In reviewing the specific security measures, it is important to recognize that we do not institute these measures without first undertaking building specific risk assessments. We are fully accountable for how we use our limited resources. Our tenants and other key partners are looking for us to be as efficient as possible by allocating limited resources where there is the greatest combination of threat and vulnerability.

We certainly encourage Congress to take a similar risk-based approach to funding homeland security. Scarce federal resources should only be allocated to places and initiatives that are addressing the greatest risk of death or injury to civilian populations.

As for lessons learned, first let me say the need for robust local communications channels with emergency response officials is perhaps the single greatest lesson learned since 9/11.

One excellent system that I believe has become a model for other cities is the New York Police Department's communication channel to the private business sector known as the Area Police–Private Leadership Security Liaison, also referred to as APPL. Information about events taking place throughout the city is now continuously provided via APPL e-mails. The recipients of these e-mails are notified, normally in real time, of events such as a manhole explosion on Fifth Avenue or a suspicious package in a Times Square train station.

This information flow allows real estate operators to ratchet up or down elements of their emergency response plans, if necessary. Equally important is the fact that we can forward this kind of information to our tenants and thus relieve frazzled nerves by reassuring them that we are in the know.

Nationally, our focus on the need for improved communications led to the development by 13 major trade associations, representing office, hotel, shopping center and multi-housing owners, for our own Information Sharing and Analysis Center, also referred to as

ISAC. Our ISAC is a 24/7, two-way information channel between the real estate industry and DHS that facilitates information sharing on terrorist threats, warnings, incidents, vulnerabilities and response planning to a network of over 120,000 real estate owners and operators.

Our best local government partners know we are looking for information, including actionable intelligence that bears directly on the operation of our buildings, and they provide it quickly. I am not sure there is any organization in the country that does a better job of this than the NYPD. By working closely over time, we have begun to have a mutual understanding of our respective roles. We know our buildings' individual vulnerabilities. Government has more of a beat on the changing threat environment. We both need each other to succeed. This is the proper model for our partnership at the federal level as well.

Another lesson learned has been the need to ensure government officials know who is actually responsible for the security of high-profile buildings in this country.

Notably at the time of the orange alert for the New York financial sector last year, the first DHS officials to communicate with the private sector about the potential risks to the Citicorp Center, including the then–Secretary of DHS, were initially unaware that Citicorp neither owned nor managed the physical security of the facility that bore its name.

To assist DHS and others to avoid that mistake in the future, the Real Estate Board of New York has made available its database of New York City commercial building owners and managers as a reference to local, state and federal officials. We strongly recommend other cities implement similar programs, perhaps working with local building owners and managers associations.

In conclusion, we are truly blessed that there have been no major attacks on our country since 9/11. However, without further incidents, it is sometimes difficult, particularly in cities that have not experienced terror attacks in the past, to ensure the proper level of realistic vigilance.

Through our ISAC, the real estate industry has recently completed a 6-month public service advertising campaign reaching well over 100,000 members of our industry. To that same end, in April, the Real Estate ISAC facilitated the participation of over 60 real estate firms in the national terrorism simulation known as TOPOFF–3.

DHS should continue to reach out to the public at large with similar awareness campaigns and to provide our industry with opportunities to participate in exercises. We will get more support for what we are doing from our key constituents if there is consensus among the general public and our industry on the need for appropriate measures.

These priorities must continue to be addressed aggressively by DHS and other government authorities. Only then can we feel confident that if there are other major acts of terrorism, we can return to your committee and say we did everything reasonably within our power to save human lives. That, in the end, is what this is all about.

Thank you.

[The statement of Mr. Norton follows:]

PREPARED STATEMENT OF MICHAEL L. NORTON

WEDNESDAY, SEPTEMBER 7, 2005

Introduction

Chairman Lungren, Ranking Member Sanchez, and Members of the Committee, my name is Michael Norton. I am responsible for managing and directing all global property management activities at Tishman Speyer. Tishman Speyer (*www.tishmanspeyer.com*) is one of the leading owners, developers, fund managers and operators of first class real estate in the world, with a property portfolio totaling more than 74 million square feet in major metropolitan areas across the United States, Europe and Latin America. Let me note at the outset that I am not aware of any Congressional hearing where owners of landmark buildings have been given the opportunity to share their homeland security experience in the post 9/11 era. Thank you then for providing this unique forum.

I am testifying today on behalf of the Real Estate Roundtable[1] (*www.rer.org*) where our company's Chief Executive Officer, Jerry Speyer, is a member of the Board of Directors. I am also testifying on behalf of the Real Estate Board of New York[2] (*www.rebny.org*) and the Building Owners Managers Association (BOMA) International[3] (*www.boma.org*) two organizations where I personally sit on senior governing boards and councils. In addition to my work with these organizations, I am active on a number of other civic and charitable organizations and was recently promoted to the rank of Lieutenant Colonel in the U.S. Marine Corps Reserves.

I. Managing the Risk of Further Terrorist Attacks on Commercial Office Buildings

A. Our Company's Stake and Commitment

The unique nature of our portfolio of assets—both existing buildings and projects under development—ensures that sophisticated risk management, including managing the risk of further terrorist attacks, is a core business priority. We own and manage some of the highest profile office buildings in the world, including Rockefeller Center, the MetLife Building and the Chrysler Center in New York City. Rockefeller Center, for example, is the number one tourist destination in New York City with all the pedestrian traffic that comes with that status. The Chrysler Center is a worldwide icon that, together with the Empire State Building, defines the New York skyline. All these buildings—and many others in our portfolio—sit atop mass transit and, in the case of the MetLife Building, Grand Central Station itself. Current projects now under development by Tishman Speyer include the new baseball stadium for the New York Yankees, a major new building for Citigroup in Long Island City, and the new headquarters buildings for Goldman Sachs and the Hearst Corporation in New York City.

In the end, our guiding principle as a company in managing the risk of terrorism is to meet or exceed the expectations of our customers—our tenants. Many of these tenants are Fortune 500 companies or other high-visibility institutions with strong commitments to managing terrorism-related risks. We are also deeply influenced by the expectations or demands of our lenders, investors, insurers, legal advisors and local, state and federal government.

---

[1] The Real Estate Roundtable is the organization that brings together leaders of the nation's top public and privately-held real estate ownership, development, lending and management firms with the leaders of major national real estate trade associations to jointly address key national policy issues relating to real estate and the overall economy. The Roundtable provides day-to-day operational staffing of the Real Estate Information Sharing and Analysis Center.

[2] As the oldest and most influential real estate trade association in New York City, The Real Estate Board of New York represents major commercial and residential property owners and builders, brokers and managers, banks, financial service companies, utilities, attorneys, architects, contractors and other individuals and institutions professionally interested in the city's real estate.

[3] Founded in 1907, the Building Owners and Managers Association (BOMA) International is a dynamic international federation of over 100 local associations. The 19,000-plus members of BOMA International own or manage over 9 billion square feet of downtown and suburban commercial properties and facilities in North America and abroad. BOMA's mission is to enhance the human, intellectual and physical assets of the commercial real estate industry through advocacy, education, research, standards and information.

B. Our Industry's Commitment

Managing the risk of terrorism in the post 9/11 environment, and I am speaking for the industry as a whole at this point, has galvanized our individual and common resources to an unprecedented degree. By our industry's standard benchmarking reference—BOMA's 2005 Experience Exchange Report [4]—we are spending, as an industry, over 20% more on security than we were pre 9/11. And yet, I hesitate to mention that statistic because in the end managing risk is not principally about allocating *additional* resources, it is about strategically using *existing* resources to cost-effectively mitigate risks. Information and experience are two assets that are hard to put a dollar value on and yet they may be the most critical resources we have. Post 9/11, there has been an unprecedented degree of information sharing within our industry and with local, state and federal counter-terrorism and emergency response authorities. This sharing of information—including best practices—is being advanced in New York City through the sophisticated local networks facilitated by the Real Estate Board of New York as well as national networks supported by the Real Estate Information Sharing and Analysis Center or ISAC (*www.reisac.org*), and the various committees and task forces of BOMA and the Real Estate Roundtable. We are also allocating substantial resources as an industry to support the work of Rand Corporation's new Center for Terrorism Risk Management Policy. (*http://www.rand.org/multi/ctrmp*)

C. The Nature, Including the Limits, of Our Industry's Role

Upon reflection, it is evident that the terrorist attacks in New York City on 9/11 were, among other things, attacks on major US commercial buildings and their tenants/occupants. In the aftermath of these events, no one has implied that the collapse of the two towers was as a *direct* result of the failure of the commercial real estate industry. In fact, just five years after the 1993 Trade Center bombing, the twin towers became internationally renowned for having the *best* security measures of any commercial real estate property in the world. After 1993, the World Trade Center had to provide the utmost security, without making that office, retail and hotel complex the equivalent of a closed military compound. In fact, as we all know, even a closed military complex—the Pentagon itself—was also unable to deter airborne attacks on 9/11.

As a result of the attacks of 9/11, the subsequent anthrax scares (including one at NBC studios, located in Rockefeller Center), last year's Citigroup Building incident, and the recent London bombings, the commercial high-rise building industry, through no failure of its own, has been severely affected, challenged, and thrust into the heart of the terror threat issue. We always look for ways to better manage the risk of further threats and attacks. But, at the same time, we remain very dependent on the ability of government (including mass transit authorities) to help limit the ability of terrorists to reach our facilities in the first place.

D. The Reality of Target-Substitution

As Frank Cilluffo, the former special Assistant to the President for Homeland Security and the current Director of the Homeland Security Policy Institute at The George Washington University, testified before this subcommittee on June 15, 2005,

> We do not face an adversary that we can defeat in a conventional war on a traditional battlefield by going plane for plane or tank for tank, but one that will take the path of least resistance by constantly searching for our greatest vulnerabilities.

Mr. Cilluffo's assessment, as well as that of many experts with Rand's Center for Terrorism Risk Management Policy, confirm the harsh reality of "target substitution." Specifically, as traditional critical infrastructure, including government facilities, are further hardened, the attractiveness and vulnerability of our nation's so called civilian "soft targets" is *increasing*. To mitigate this disturbing reality, it is crucial that we move to *simultaneously* address the threats against both hard and softer targets.

E. Pre-condition for all Security Measures: Sound Risk Assessment

Before detailing specific risk mitigation measures, it is important to stress the central role that building-specific risk assessments play in any rational allocation of resources. We are fully accountable for how we use our limited "resources". Our customers, lenders and investors are looking for us be as efficient as possible.

---

[4] The Experience Exchange Report is an annual income and expense benchmarking report for the commercial real estate industry performed by the Building Owners and Managers Association International for more information see www.boma.org. The report is based on the weighted average responses of 3,210 buildings, representing approximately 700 million square feet of space.

Spending more of their money, while sometimes appropriate, is not the way that we or our constituencies measure progress. Limited resources need to be applied first to those measures that have the greatest potential for limiting loss of human life and property damage.

Risk is assessed both from the standpoints of threats and vulnerabilities. In addressing the vulnerability-part of the equation, we have benefited (as I know other major real estate companies have been) by visits from DHS officials that have reviewed with us our own assessments of our properties' vulnerabilities. These teams toured a number of our buildings and spent a day at each property, speaking with the staff and assessing what security measures were in place and what additional measures we might consider now or in the event of specific threats. We understood the overall aim of this exercise for DHS was to assess privately owned commercial office buildings across the country in an effort to establish the current state of security at these high profile locations and to identify what "best practices" can be established and shared among our business community. The DHS visits were informative exchanges of private and public sector perspectives and helped establish improved working relationships between our organizations. In New York, the NYPD provides a similar service.

II. Commercial Real Estate Industry Lessons Learned and Best Practices for Managing Terrorism Risk for Higher-Risk Buildings

The specific "lessons learned" and examples of best practices I would like to share now with the subcommittee fall into six basic categories: communication, emergency response (including emergency area access), training programs, "hardening" techniques, information sharing, and coordination initiatives.

A. Communication & Information Sharing

One of the greatest lessons that the real estate community learned from 9/11 was the need for more robust communication channels between the private and public sectors. These channels—both formal and informal—should enable real estate operators to instantaneously receive information and act more effectively based on that that information. The channels should convey valid information, as well as dispel rumors.

Locally: The need for robust local communications is perhaps the single greatest lesson learned since 9/11. One excellent system—that I believe has become a model for other cities—is the New York Police Department's communications channel to the private business sector known as the Area Police-Private Leadership Security Liaison or "APPL."[5] Information about events taking place throughout the city is now continuously provided via APPL emails. The recipients of these emails are notified normally in real time of events such as a manhole explosion on Fifth Avenue, a suspicious package in a Times Square train station, or an unauthorized helicopter flight over the Empire State Building. This information flow allows real estate operators to ratchet up or down elements of their emergency response plans, if necessary. Equally important is the fact that we can forward this kind of information to our tenants, and thus relieve frazzled nerves by reassuring them that we are "in the loop."

After this communication channel was established with the NYPD, Tishman Speyer subscribed to an international communication service that enables us to send messages to employees and tenant contacts worldwide via email, text messages, and voice messages. Here is a real-world example of how this information flow helps our company operate more effectively:

> Last month a suspicious package was discovered against a building located on 54th Street and Madison Avenue, which is directly across from one of our properties. The police had arrived and closed off all pedestrian and vehicular traffic. APPL sent out a message that informed us what was occurring and later notified us that the package was found to be a regular briefcase with no explosive devices. We were then able to use our own in house multi-medium communication channels to simultaneously inform every one of our tenants.

---

[5] A number of other cities have strong systems in place or under development. In Chicago's Central Business District the Chicago Police Department has established the Security Broadcast Email System to communicate with private sector security directors. Within the same district they have established the Early Alert Radio Network (EARN) program. EARN is a system by which high-rise buildings that purchase a radio receiver can obtain information from the Chicago Police Department. In the District of Columbia, "D.C. Alert" uses the Roam Security Alert Network (*https://textalert.ema.dc.gov/index.php__*CCheck=1) to provide immediate text notification and update information during a major crisis or emergency. This system delivers important emergency alerts, notifications and updates to a number of devices, including cellular telephones, e-mail accounts, Blackberry© devices, and pagers.

Nationally: The real estate industry—including major office, hotel, shopping center and multi-housing owners and operators—has requested and received permission from federal counter-terrorism officials to create our own Real Estate Information Sharing and Analysis Center (ISAC). The ISAC is a 24/7, two-way information channel between the real estate industry and DHS that facilitates information sharing on terrorist threats, warnings, incidents, vulnerabilities and response planning to a network of over 120,000 real estate owners and operators. For many years prior to 9/11, traditional critical infrastructure industries (e.g., the financial services, electric power, oil and gas, water, telecommunications, information technology, chemical and food industries) all operated similar ISACs. We are grateful to the White House and DHS officials that were willing to think "outside the box" by supporting the creation of an ISAC for our industry.

B. Emergency Area Access Procedures

Another lesson learned was the need for essential authorized building personnel to have access to their properties as soon as possible following an event. Immediately following the September 11 attacks on the World Trade Center the police cordoned off a very large area in downtown Manhattan. However, in the future, property managers and building engineers, who can identify themselves as such, will be granted access to these types of restricted areas in order to address vital building issues (e.g., shutting down running machinery and turning off water lines). This will allow us to prevent any additional damage and further economic loss. The cities of Boston, New York, and Chicago have all instituted programs that allow private property owners to register critical personnel with the city for that purpose.

C. Training Programs

Another lesson learned is the importance of expanding training programs that incorporate the lessons learned from 9/11 so that they can better prepare security officers and building management officials that work in high-rise office buildings. Training should address not only evacuation procedures, but also consider the difficult issue of how and when to "shelter-in-place" if an actual or suspected bio-chemical event occurs.

The American Society of Industrial Security, International (ASIS, International) has established the Private Security Officer Selection and Training Guideline. This guideline sets forth minimum criteria for the selection and training of private security officers, which may also be used to provide regulating bodies with consistent minimum qualifications. In addition, ASIS's Physical Security Measures Guideline is currently under development. This guideline will assist in the selection of appropriate physical security measures, including defining risk levels, implementing an integrated set of physical security measures, and devising policies and procedures related to security incidents, access control, monitoring systems, lighting, security personnel, and audits and inspections. When completed, this will be an extremely helpful tool to ensure that we members of the private sector are providing improved training to our security officers and other relevant officials.

Training should be provided not only to security officers but also to other building personnel, including property managers, engineers, fire safety directors and cleaners. It is important to remember that, for all these groups, emergency action plans should be considered crucial elements of their respective training programs. Exercises that test these action plans are fundamental to the learning process. The training, should, of course, include how to address biological and chemical attacks, explosive devices, suicide bombers, and other recognized terror techniques.

D. Target Hardening Techniques

As discussed above, it has become common practice, as part of sound risk assessments, to perform vulnerability risk assessments on all major properties. Buildings that receive high threat vulnerability ratings may be appropriate for target hardening especially against explosive devices (vehicular or pedestrian borne). Target hardening focuses particularly on building lobbies, and since 9/11 many large commercial office buildings in New York have installed turnstiles and card access readers. In addition to the lobbies, the facades, loading docks, and underground parking lots of many commercial office buildings have been target hardened. After 9/11, Tishman Speyer target hardened various elements of all of its then existing properties We are also developers and as such we now incorporate target hardening from the very beginning of the design and construction process.

E. Research

As stated above, post 9/11, the commercial real estate industry has supported sophisticated research on how best to protect our homeland. Most notably, we have helped launch the new RAND Center for Terrorism Risk Management Policy (CTRMP) and provided high-level technical consulting to that organization. While

the Center has several missions, one of its principal goals is to help security decision-making in an age of catastrophic terrorism. Its mission is to help not only the private sector but also the public sector assess the consequences of individual and collective decisions about allocating terrorism security resources and help these institutions make decisions about the risks they face and the security portfolios appropriate to mitigating those risks.

In addition to analytic research, the CTRMP has provided invaluable learning tools for interactive strategic exercises. Most recently, CTRMP further developed a RAND simulation involving the mock detonation of a nuclear device smuggled into the United States aboard a container ship in a major California port city. The exercise, which was developed for various business sector audiences and senior Congressional staffers, showed just what the human and financial losses would be if this were actually to occur and what impact it would have on other parts of the United States and the rest of the world.

F. Coordination with Government Authorities on Building Ownership and Management Data

The commercial real estate industry stepped up to face another challenge last summer when the national threat advisory system was elevated for the financial sector. As you know, intelligence was uncovered showing al-Qa'ida was doing extensive pre-attack surveillance on prominent properties housing several major financial institutions. The Citicorp Building in New York City was one of those properties. Notably, the first DHS officials "on the ground" in New York—including the then Secretary of DHS—were initially unaware that Citicorp neither owned nor managed the physical security of that facility. Indeed, across the country, it is not uncommon for counter-terrorism officials to assume that the companies whose names are associated with landmark buildings actually own or manage those buildings.

To assist DHS and others identify quickly those actually responsible for the management of a given building's physical security, the Real Estate Board of New York has made available its database of New York City commercial building owners and managers as a reference. This database is regularly updated as purchases and sales take place within the New York City office market. It includes landline telephone, cellular telephone, beeper, and email contact information sorted by building name and address. This could prove to be a valuable resource for DHS, especially when notifications are required in an "actionable" timeframe. REBNY has also provided this database to the New York City Office of Emergency Management (OEM) and to the New York City Department of Buildings (DOB). We encourage other cities to make use of similar data bases of office buildings by working with local BOMA organizations.

G. Building Industry Awareness Through Media Campaigns and Exercises

Post 9/11 it has become increasingly clear that without continuous citizen awareness campaigns, public interest and concern about terrorism can drop dramatically. This is particularly true in cities that have never had a major terrorist incident. Therefore, the Real Estate ISAC in January of 2005 commenced a six-month public service advertising campaign to encourage building owners and managers to address homeland security issues. Through their "Fighting Terrorism" advertising campaign in *Real Estate Forum* and 10 trade journals, the ISAC, its trade member groups and its media partner, Real Estate Media Inc., have reached over 120,000 real estate professionals with their important message about the need for a well-prepared real estate industry sector.

To the same end, in April, 2005, the Real Estate ISAC further advanced its mission of encouraging greater industry awareness and readiness by facilitating the participation of over 60 real estate firms in the national terrorism simulation exercise known as "TOPOFF 3". This biennial exercise, involving some 10,000 federal and state officials and representatives of Great Britain and Canada, sought to strengthen the nation's capacity to prevent, prepare for, respond to, and recover from large-scale terrorist attacks involving weapons of mass destruction. It was the first of these exercises in which the private sector, including the commercial real estate sector, was allowed to participate on an equal footing with our public sector partners. Those who participated from our industry leveraged this multi-million dollar federal exercise to assess their own current emergency plans. Following the exercise, industry participants reported making changes to those aspects of their plans that were found to be insufficient. Going forward, I cannot stress enough the importance to our industry of opportunities to participate in joint exercises with local, state and federal officials.

H. Specific Security Measures and Best Practices for Major Buildings

In our company's experience, effective building security is a combination of design features (e.g., physical barriers and electronic systems), personnel and staffing strategies (personnel and procedural) that are integrated into a well-defined program. As indicated above, determining the degree to which each of these components should be utilized depends on several risk factors. These factors include whether the building is a symbol or has some other national status, the specific environment at or around the building (e.g., is it a tourist attraction? Are their high-risk tenants or other specific risk factors?), and the structural design of the building (e.g., is there interior parking). I would like to take a few moments to tell you about some of the security measures that have been implemented in our industry. I will use some examples of security measures that Tishman Speyer has employed at its properties, but most of these are recognized as best practices by other major owners in our industry.

- *Satellite Telephones:* Many real estate owners and operators have satellite telephones in each region where they have properties. In the event of an emergency, when all landline and cellular connections are busy, these portable satellite telephones will continue to operate. As events unfold in a region, security directors and senior managers can remain in contact with personnel on location in order to assess the situation and issue instructions. The satellite telephones also ensure that the building staff will be able to communicate with the emergency services at all times during an incident. Furthermore, key personnel, including senior management, should carry emergency contact information with them at all times.
- *Emergency Procedure Guidebooks:* Buildings are often equipped with Emergency Procedure Guidebooks These standardized manuals provide staff members with check lists of their respective responsibilities in the case of a property emergency. This ensures that, even under difficult circumstances, building personnel will know the procedures necessary to facilitate the safe evacuation of their properties.
- *Company or Building Specific-Color Coded Alert Systems:* Many real estate companies have instigated their own internal color code or security level alert systems. For example, under our procedures, the color green represents the current "Standard Operating Procedures", the color yellow indicates "Heightened Alert Operations" and the color red signifies "Emergency Event Operations." This system requires us to constantly and consistently assess the security risk in any region at any time.
- *Emergency Response Training Videos:* Tishman Speyer has developed a two hour training video for property staff to learn about biological and chemical agents, including their effects on the human body, how they can be transmitted, and what initial actions should be taken while waiting for emergency services to arrive. The objective of this training program is to help ensure that the property staff can better identify the potential release, dissemination, or detonation of these deadly agents in the event of an attack. This training segment also addresses what actions may be appropriate to take once an attack has occurred, including evacuations or sheltering in place, shutting off of fresh air intakes, and receiving of updates from the local authorities.
- *Terrorism Awareness Training:* Security officers also receive training in terrorism awareness and response. The elements of common terror attack modes are discussed with a focus on the opportunities a security professional may have to intervene. The officer is encouraged to concentrate on a person's behavior, as opposed to a person's physical characteristics. For the purpose of this training, the "Stages of a Terrorist Event" are defined as "Target Selection; Surveillance of the Target; Planning of the Operation; Rehearsals and Dry-runs; Escaping from the Target; and the Exploitation of the Act." Finally, substantial time is committed to discussing conventional explosive devices and improvised explosive devices, as well as the correct way to handle a report of a "suspicious package" or telephone or written bomb threat. This kind of in-house training may be supplemented by DHS's own "soft target" terrorism awareness training programs.
- *Rapid Shut Down of Air-Intakes:* Some high profile buildings have implemented controls that enable building personnel to quickly and easily shut off the fresh air intakes in the case of an emergency. Automatic shut-off switches have been installed at appropriate locations and can easily be activated if we receive timely information from the relevant authorities. A critical aspect to successfully addressing a potential biological or chemical agent attack/event at or in the vicinity of a building is having adequate early warning/communication channels with the appropriate local government.

• *In-Depth Property-Specific Threat Vulnerability Assessment:* In our high profile properties property specific threat vulnerability assessments were performed by nationally recognized security consultants, and these consultants provided recommendations on how to improve security in certain areas. Action plans to implement these recommendations, together with the corresponding budgets, are formulated by each individual building's property manager in light of property specific factors including tenant demand.
• *"Closed Buildings":* Many properties that are viewed as potential targets have been transformed from open access buildings into "closed" buildings. Building lobbies were historically vulnerable areas for unauthorized access into a facility. Without lobby access control, anyone can enter an elevator and reach any floor desired. Prior to September 11, 2001, most properties only enacted access control systems after normal business hours (6PM—7AM, Monday—Friday and weekends). Since 9/11, turnstiles and visitor pre-registration systems have been installed in certain buildings to provide management with detailed knowledge of when people are entering the property. In order to pass through the turnstiles, tenants must have valid building-issued identification cards including personal photographic images.
• *Visitor Processing Centers and Courier Centers:* Post 9/11, some buildings have set up visitor processing centers and courier centers. The visitor centers authorize access to the elevators only after they have received approval from relevant tenant hosts. The security officers then scan the visitors' proof of identification and issue temporary access badges, in some cases with photographs of the visitors on them. At the courier centers, security officers use X-ray machines to scan all packages. In some cases, couriers are not granted access to the buildings and instead building employees deliver packages to the appropriate offices.

H. Response to the London Mass Transit Bombings

The London bombings occurred exactly two months ago to the day, on July 7, 2005. As such, it is still too early to identify exactly what new lessons we learned and what new security measures will be instituted as a result of this tragedy.

We have long had an excellent working relationship with the Metropolitan Transit Authority (MTA) and are working with the REBNY and the Real Estate Roundtable to build a stronger industry-wide partnership with mass transit authorities throughout the nation. We are, of course, also watching closely as the MTA looks at the benefits of increased use of CCTV. This is one example of how this nation appears to be embracing technological advances to increase the safety of our civilian infrastructure. This is particularly relevant to us as we need to provide tenants with secure buildings but also we are directly affected by our tenants' confidence in the public transportation that delivers them to our properties on a daily basis. Furthermore, as I mentioned at the outset, many of our properties are built directly above subway networks and we are only as secure as our weakest link. Again our dependence on sound government security initiatives is extraordinary.

III. Continuing Challenges & Policy Recommendations

My testimony has stressed specific "on the ground" lessons learned and best practices with the hopes that this may spur dialogue within our industry and elsewhere on how best to encourage improved homeland security. I recognize the extraordinary challenges that local, state and federal government authorities face in helping to advance the state of the art in terms of homeland security. At the same time, as an industry, we do have some policy suggestions for you to consider as you oversee the work of DHS.

A. Priorities

Emergency Response: In terms of allocating scarce federal resources, when it comes to improving public-private homeland security partnerships, we agree with the emphasis the 9/11 Commission has placed on the need for emergency response and business continuity planning. In that regard, we believe that partnerships *at the local level* with emergency response agencies should be a top priority. DHS can and should continue to support—financially where appropriate—outreach efforts at the local level to bring the business community more fully into partnerships with local emergency response officials. The decision to spend very limited federal funds should be made with a very realistic understanding of the different level of threat and vulnerability presented by different geographic locations.

Also with respect to emergency response planning, we are well aware of the spotlight the 9/11 Commission, and later federal legislation, placed on the general goals and principles set out in the National Fire Protection Association Standard on Disaster/Emergency Management and Business Continuity Programs (NFPA 1600). As

an industry we have a range of sound references to help us begin to apply those very general goals and principles to specific buildings and situations. As you may know, that Standard was not developed with individual building issues in mind.

It will be important to retain the flexibility to make asset specific decisions, based on asset specific risk assessments. At the same time, we recognize the need to encourage greater consistency of performance across all business sectors and within our sector. The government does have a role in helping to create a shared language and set of performance oriented metrics in this area. We look forward to working with DHS and others to help improve the private sector's emergency readiness. A solid simulation and exercise program at the local level—supported where necessary by federal resources—is an important step in this direction. We also suggest that DHS continue to work closely with the insurance industry to ensure their policies offer proper incentives for positive performance in the area of emergency response planning.

B. Actionable Intelligence

With respect to the issue of intelligence sharing with the private sector, I want to stress that we are not asking for uncensored access to all intelligence reports. What we are looking for is access to any information made available to local counter-terrorism officials that bears directly on the operation of our buildings. Where the threat is so vague and general that no "actions" are being recommended, that fact also needs to be made clear. As indicated above, we have a growing number of strong partnerships at the local level where intelligence is shared effectively with our industry. I am not sure there is any organization in the country that does a better job of that than the NYPD. By working closely over time, we have begun to have a mutual understanding of our respective roles. We know our buildings' individual vulnerabilities; government has more of a beat on the changing threat environment. We both need each other to succeed. This is the proper model for our partnership at the federal level as well.

C. Public Awareness

Often, conflicting tenant expectations and awareness are challenges that we face as an industry. The tenants want to be comfortable that we are doing everything possible to ensure their safety but at the same time they do not want to work in a military fortress. We note that striking the right balance in this regard is also an issue that the public transportation authorities are forced to deal with today. The DHS needs to support the efforts at the local level to build public and business awareness of the importance of proper planning and training in this area. Only when our tenants have fully "bought-in" to the importance of this issue do they support our efforts to take rational security measures. In many parts of the country, tenants do not believe this issue is a major risk factor and are therefore unwilling to pay for some or all of the specific measures, I've detailed above. In my view, government has an obligation to help educate the public in a reasonable and realistic way about the threats we face in the post 9/11 environment. Frankly, unless or until there are more attacks, that educational process will be very challenging. Hearings like this and recent public comments by Secretary Chertoff suggest top government officials are committed to this goal.

Conclusion

These priorities must continue to be addressed aggressively by DHS and other government authorities. Only then can we feel confident that, if other major acts of terrorism were to occur, we could return to your committee and say we did everything reasonably within our power to save human lives. That, in the end, is what this is all about.

Thank you and I am happy to take questions.

Mr. LUNGREN. Thank you very much, Mr. Norton, for your testimony.

The chair would now recognize Mr. Joe Madsen, director, safety and risk management for the Spokane Public Schools, to testify.

Thank you for coming, sir.

STATEMENT OF JOE MADSEN

Mr. MADSEN. Chairman Lungren, members of the Committee, I am Joe Madsen. I am a risk manager in a school district of 31,000.

There are 47 million students every day attending schools in our nation. Of those, 25 million ride 444,000 school buses. They do over

8.8 billion trips and are exposed that many times per year in regards to them being a soft target.

I have provided you written testimony indicating what we in Spokane have done with the school district, the fire department and the police department.

I certainly could come before you to indicate our wants, needs and desires in terms of funding for facilities, for training, target-hardening, or specific allocations for school resource officers. I, however, think it is more important to concentrate on the big picture, those things that actually matter at the ground level; those things that have affected us in Spokane.

The all-hazards approach that we have conducted affects not only terrorism, not only disasters, or natural disasters, but any type of incident and the planning and preparation for those in advance has been what made the difference for us. Potential issues such as critical incidents, natural disasters and of course terrorism are those issues that we need to concentrate on.

We are a nation of special interests, but one that cannot be seen through only one set of lenses. We need to be constantly looking at the big picture and looking at systems approaches, systems which combine resources, shared data, relationships built on trust, joint training exercises, not just large-scale required drills, but small-scale trust-building exercises. It is less about me and mine, but more about us.

Systems revolving around communications, relationships, preplanning, data-sharing and the use of technology, I am here to tell you that it can be done with successful results.

In a microcosm, I manage five departments: safety, transportation, security, worker comp, and insurance. Those five departments 10 years ago did not work together. They reported to different people and they did not help each other. But over the last 10 years, we have been able to cause the effect that we need to successfully work together.

By ensuring that safety officers work with security officers, that security officers work with transportation staff, we ensure a system that responds to an incident no matter large or small, no matter whether it is a security issue or a safety-related issue, as a unit.

In the city of Spokane, we also have made that opportunity. For over 10 years, we have had police liaison meetings between the school district and the police department. Those types of relationships and trust-building are critical to having resolved our incident at Lewis and Clark High School.

Just 2 weeks ago, the police department conducted SWAT exercises within our high schools. They did not do it by themselves. They did not do it at the police academy, but they came into our schools. They have been doing this for years. At those exercises, we had our principals and our district resource officers.

It is the relationships that we have built over the past several years that allow us to respond to an incident, to plan for it, and to communicate effectively when an incident occurs.

At the state level in Washington, we have the Department of Emergency Management, the Office of Superintendent for Public Instruction, the Washington State Patrol, all working together with a data management system that allows us to map schools, to pro-

vide photographs, to provide the information related to the critical structures and information related to the organizational charts in every one of our facilities.

Right here today in my computer, I have all 12 of our high schools and middle schools and all the data I need to make a decision from across the nation to be able to respond to an emergency or to communicate effectively with the fire department and police department.

It is communication, relationships, data-sharing, preparation and working together as a system that causes the effect that we need. The question is, is on the federal level, are we sharing data, are we communicating, and do we have the relationships between the multitude of different agencies?

I work currently with the Department of Homeland Security, the Department of Education, Occupational Safety and Helath Administration (OSHA), but I receive different direction from each of them. If we can have the relationships and the information and the communication that I think that we have shown in Spokane in the state of Washington with our police and fire, I think that we would go a long ways to solving our issues such as Katrina.

Thank you for the ability to present. You have my written testimony. I would be happy to answer any questions.

[The statement of Mr. Madsen follows:]

PREPARED STATEMENT OF JOSEPH C. MADSEN

WEDNESDAY, SEPTEMBER 7, 2005

Mr. Chairman, Ranking Member Sanchez, and Members of the Subcommittee, thank you for having me here to discuss this important subject. My name is Joe Madsen and I am the Director of Safety and Risk Management for Spokane Public Schools in Spokane, Washington.

I am before you today to discuss school safety and how the federal government can be more proactive in protecting our school children, teachers, and staff from a wide variety of threats and emergencies. Following 9/11, the federal government focused its efforts on improving security around airports, transit systems, and public facilities, the so called "hard targets." Today I'd like to talk about one of our nation's most valuable assets, our children, and a successful program begun in Washington State that combines old fashion relationship-building, interagency cooperation, and state-of-the art technology to protect our schools against terrorist attacks and other emergencies.

We have more than 47 million children enrolled in educational facilities across the U.S. Because schools typically contain large numbers of students in a single location, they represent an appealing target for terrorists seeking the maximum emotional impact for their cowardly acts. Domestically we've already experienced a form of terrorism, and schools like West Paducah in Kentucky; Springfield in Oregon; Columbine in Colorado; and Red Lake in Minnesota stir emotion in the hearts of parents and dispel the feeling "that it couldn't happen here." On the international side, it's even more disturbing. In Beslan, Russia last year, terrorists took more than 1,100 hostages at a local school. More than 330 students and staff were killed and another 700 people were seriously injured. A similar incident occurred this June when terrorists attacked an international school in Cambodia and took over 70 children and staff hostage.

I know first hand the damage a terrorist attack can do at a school. At 11:30 a.m. on September 22, 2003 a student with a 9mm handgun entered one of my schools, Lewis and Clark High School, in Spokane. It was the lunch hour and the school was packed with more than 2,000 students eating lunch in the hallways, a tradition at this school.

Normally, chaos would break out at this point. But in Spokane, the police, fire, school staff, and students are well trained on how to respond to emergencies. Just prior to the incident, Washington State had begun deployment of a statewide crisis management system (CMS) for protection of critical public infrastructure. Using this

new system, the Spokane Police Department, the Spokane Fire Department, the Washington State Patrol, and school district officials implemented pre-determined tactical response plans and quickly responded to the school. Detailed information about the school building in the CMS system allowed police to isolate the gunman in just 12 minutes, evacuate more than 2,000 students to a pre-established family re-unification center, and immobilize the gunman. The students were spared the trauma of having to witness the incident and were able to return to their school the very next day.

This situation, and it would be no different if it had been an organized terrorist incident, a fire, a hazmat spill, or a hurricane, was successfully mitigated because the first responders in Spokane have developed an excellent system for emergency response, involving training, relationship building, implementation of FEMA's National Incident Management System (NIMS) protocols, and use of state-of-the art CMS technology that makes critical facility information accessible to all responding agencies. How this incident was handled, and the systems put in place to mitigate such events, could well serve as a model for other school districts across the nation.

I'd like to take a few minutes to talk about this incident in greater detail, because the story exemplifies many of the issues facing police and fire today in responding to a wide variety of emergencies.

To provide you with some background: In 2003 the State of Washington funded development of a statewide crisis management system for critical infrastructure. The computer-based system provides first responders with instant access to critical information, including fire and police tactical preplans and more than 300 data points including facility emergency plans, satellite images, interior and exterior photos, floor plans, evacuation routes, utility shut-offs, hazardous materials locations and more. The simple, easy-to-use software is designed to allow emergency response personnel to act quickly, decisively, and safely during any facility-related emergency incident. The system combines data that used to be kept in three-ring binders at a variety of locations into a single, master database. It also provides all responding agencies with equal access to critical infrastructure data. Equally important, facility owners can quickly update information about changes at their facilities via the Web, ensuring that first responders are basing their decisions on the most current data available.

This system was implemented at Lewis and Clark High School in August 2003, just two weeks before the actual shooting incident. An integral part of the implementation is a series of planning sessions where school officials meet with their local police and fire representatives to pre-plan how each agency will respond to various emergency scenarios. This process establishes working relationships between first responders from various agencies and is the basis for development of trust and cooperation. The system is also compliant with FEMA's National Incident Management System (NIMS) and the Incident Command System (ICS). ICS, a subset of NIMS, is a standardized on-scene incident management protocol designed to allow responders to adopt an integrated organizational structure equal to the complexity and demands of any single incident or multiple incidents without being hindered by jurisdictional boundaries.

The crisis management system adopted by Washington State melds well with the approach advocated by many of our nation's police and fire departments emphasizing the primary role local public safety agencies play in emergency response:

1. Local responders need to have venue specific information available to them in order to plan, prepare, and mitigate acts of terrorism and other emergencies (both man-made and natural).
2. While not frequently addressed in national anti-terrorism policy, schools represent perhaps our community's most sensitive venues.
3. Local, tribal, state, and federal public safety providers need to have affordable, reliable, scalable, and extensible data system(s) to manage this information.
4. Development of "information silos" creates interoperability issues at local, regional, and federal levels. The goal would be development of a standardized national interface.
5. First responders need to have simple and reliable access to information in order to act swiftly and decisively.
6. Disaster mitigation requires interagency cooperation and common access to information in a standardized form.

The Lewis and Clark High School Shooting Incident

Now, let's go back and look at how this combination of interagency cooperation, preplanning, use of the Incident Command System protocols, and implementation of a crisis management system helped us successfully mitigate a potentially dan-

gerous shooting incident at Lewis and Clark High School. It is important to remember that during this type of incident, many things are happening concurrently and involving a wide number of public safety agencies and other stakeholders.

As gunfire rang out in the school, the principal and the school resource officer (SRO) immediately responded to the 3rd floor to evaluate the situation and determine the exact location of the gunman. In a shooting incident, the standard operating procedure calls for a school lockdown, but in this situation there were thousands of students out in the hallways eating lunch. After a short discussion, they realized the quickest way to evacuate the students was to pull the fire alarm. Lewis and Clark students go through numerous fire drills during the school year and were quick to respond.

At the same time, a SRO at another school had pulled up the crisis management system on his laptop and was relaying information about the gunman's location and the school layout directly to police dispatch, which in turn passed the information on to responding officers.

Local patrol officers arrived at the school within four minutes and initiated what is known as an "active shooter response" to contain the suspect. This means that they immediately entered the school and moved directly towards the gunman, not waiting for a SWAT team to arrive and deploy.

During the Columbine incident, it took more than five hours before officers responding from multiple police agencies coordinated their efforts and entered the building.

Fire, police, and school security quickly set up a command post in a pre-determined location and accessed the crisis management program on a nearby computer. The program can be accessed via laptop computers, Internet connected computers, or by thumbnail-sized USB devices carried by SROs and first responders. A SRO initially assumed the role of Incident Commander per the ICS protocol. Police, fire, and emergency services in the Spokane area all adhere to ICS, whereby responders play pre-determined roles during an emergency, independent of their rank or agency. This high level of coordination made a world of difference in their ability to quickly respond and mitigate the critical situation at the high school.

The SWAT team, taking over from the active shooter team, positioned themselves in a nearby stairwell outside of Room 307 where the gunman was barricaded. They were puzzled when he popped his head out of three different doorways along the 3rd floor hallway. Officials at the command post accessed the floor plan via the CMS system and told them that Room 307 and Room 305 were connected by an internal doorway.

As a hostage negotiator began talking with the gunman, officials in the command post noticed that the corner room he occupied had unobstructed views of the grassy field where the students had been evacuated, and to eight lanes of traffic on the adjacent Interstate 90 freeway. Officials viewed aerial photos of the site and decided to move the students under the overhead freeway where they would be out of the line of fire. Using phone contacts listed in CMS, I called our transportation contractor, Laidlaw Educational Services, and asked them to immediately send 20 buses to relocate the students to an alternative site. Since the school district transportation department had participated in the preplanning sessions, they immediately understood what was needed. At the same time, a list of pre-determined roadblocks from the CMS was sent to the Spokane City Streets Department to block access to the school. Another list was sent to the Washington State Patrol to block access to the eight lanes of Interstate 90, which were exposed to the gunman's line of fire from the corner classroom. In both instances, valuable time was saved because all the roadblocks were determined during the pre-planning sessions with school officials, police, fire, and State Patrol that are part of the CMS implementation.

As news of the incident spread to parents via cell phone calls from their kids, it became important to discourage parents from driving towards the school and blocking local access routes for emergency vehicles. PIOs from both the school district and the police departments worked together to provide ongoing information to parents and the general public regarding the evolving situation.

Another problem developed when the gunman asked the police negotiator for matches. Fire officials knew from the CMS that Room 307 was a science lab, and as such, had a number of natural gas outlets. The concern was the gunman may be suicidal. In addition, there was always the potential for an explosion caused by any errant gunfire. Officials in the command post called the local gas company, which dispatched the nearest crew to help shut off the gas. Unfortunately, the crew was used to working on residential facilities and wasn't familiar with commercial installations.

Using the CMS, officials printed out photos of the utility shut-off valves and their location. A police officer escorted the utility crew and the gas was quickly shut-off. Fire officials also used the CMS to print out a list of all chemicals stored in Room 307. The printout listed the type of chemicals, their location, quantity, and Material Safety Data Sheets (MSDS) that profiled the chemical's characteristics and safety precautions.

With all the students safely evacuated, the roads blocked off, and the gunman isolated to a single location, it became a waiting game between the police and the gunman. Unfortunately, the gunman chose to provoke the SWAT team who were forced to fire in self-defense. The wounded student was quickly evacuated by waiting paramedics to a nearby hospital where he eventually survived his wounds.

What was learned as a result of this incident that is pertinent to terrorism incidents and other emergencies? First, schools are highly vulnerable to a terrorist type attack. They need to be considered by DHS for both increased funding and protection. Secondly, in any such incident, local responders always will be the first on the scene. In even a minor emergency, these responders will represent multiple agencies with overlapping and sometimes divergent priorities. It is absolutely critical that these agencies establish trusted, working relationships with each other prior to a major event. Facility owners (schools, court houses, businesses, etc.) also need to sit down with public safety officials to talk about how they will respond to a wide variety of emergencies, and how they will work with other agencies to mitigate the situation. Third, agencies need access to common, pre-established communications channels during emergencies. Last week's rescue operations following Hurricane Katrina emphasize the problems when public safety and other responders cannot communicate with each other during rescue and recovery operations. And lastly, all first responders need access to detailed, up-to-date building and site information, such as that provided by a crisis management system.

The Problem of Protecting Students on School Buses

I've talked about the procedures for protecting students in school buildings, but we also need to consider the problem of protecting students on school buses, an often neglected area in emergency plans. Spokane Public Schools serve 31,000 students in 55 different facilities, including six high schools, six middle schools, 35 elementary schools and a variety of special schools located in jails, hospitals and contracted agencies. Seven thousand of these students ride school buses to get to and from their local school. These 167 buses, carrying between 44 and 72 students each, travel 9,000 miles each day, the equivalent of going from Spokane to New York City and back 180 times a year. Along the way, they stop at thousands of bus stops to pick up children.

To give you an idea of the scope of the problem, there are more than 47 million students in any given day attending our nation's schools. Of these, 25 million ride in 440,000 yellow school buses that travel *8.8 billion trips each year.* This is in comparison to public transit systems that serve 5.2 billion unlinked passenger trips each year in the U.S.

It is now easy to understand why protecting students on all these buses is a gargantuan task. Imagine this frightening scenario: One of the Spokane School District buses does not show up at its school of destination after picking up its 58 students. It takes 12 minutes until a phone call is made from the school to the transportation department. They in turn call the bus contractor who attempts, without success, to contact the bus by radio. After another 15 minutes, the school district's security department and the Spokane Police Department are notified. In a city of more than 150 big, yellow school buses, it is next to impossible to check each one to see if they are the missing school bus.

Meanwhile in Miami, Florida; San Francisco, California; Dallas, Texas; Tupelo, Mississippi; and Mt. Lebanon, Pennsylvania the same scenario is unfolding. Each local jurisdiction is dealing with a crisis of a missing bus full of children. It isn't until an hour later that a connection is made by a national AP reporter who ties together news reports of three of the instances. Thirty minutes later, now two hours into the incident, it is confirmed by an anonymous phone call to the FBI that what was a series of localized emergencies is now a national terrorist crisis.

While it would be impractical to provide armed escorts for the thousands of school buses on our nation's roads each day, we can use technology, training, and communications tools to better protect these children. One solution, being implemented in Spokane Public Schools, is to do "security mapping" of school buses and incorporate this information, along with tactical response plans, into a CMS system. A similar approach could be taken with our metropolitan transit authorities nationwide, many of whom provide transportation services for school children.

Constant Shifting of Priorities Jeopardizes National Security—A Study of HVAs

Another issue effecting national security is how Hazard Vulnerability Analysis (HVA) information is "siloed" and not shared with other agencies. HVAs have been and continue to be a vital means of studying and prioritizing local community, state, and national areas of concern regarding natural disasters, emergencies, and security crises. There is no question that HVAs should be conducted at the local, state, and national levels. That said, local agencies, including emergency responders such as police, fire, medical, and EMS, as well as the institutions they serve (school districts, businesses, hospitals, etc.) should be held responsible for response planning, training, facilities security improvements, etc.

Equally important is that the HVAs utilize an "all hazards" approach. I feel HVAs should not focus solely on security issues at the expense of fire prevention, medical services, or hazardous chemical exposures. As Hurricane Katrina has shown us in the past week, whether it is a terrorist incident, a hurricane, a flood or any other type of disaster, the emergency response is similar in all cases. Emergency agencies, as well as businesses and institutions, should support the cooperative sharing of HVAs through communication and joint planning.

The root of this problem is that agencies often operate within a vacuum of their own priorities, frequently at the detriment of other agencies or service providers. Nationally, we seem to be bouncing from one priority to another (air transportation to subways to trains, etc.) with little coordination between agencies, first responders or those affected. HVAs certainly help to set department goals, budgets, training, etc., but if done without consultation with other responder agencies, it creates a system of individual priorities, and often, conflicting priorities. As a result, decisions about finance, training, personnel, equipment, policies, and response procedures are made without dovetailing into a national priority. It is easy to get caught up in MY needs and priorities when in an emergency; WE will need to work and act together as a system.

The Importance of Sustainability of Programs

Often the sustainability of a program is only thought of in regard to the funding of the program. Sustainability should be tied to local community priorities, or decisions regarding the determination of HVAs made by all stakeholder organizations. It is only through this joint decision-making that long term support of a program can be ensured. Most federal grants now require the signatures of many different service agencies or end users. These signatures by themselves, however, do not ensure long term cooperation.

Another aspect of sustainability is the continued "silo effect" that permeates many agencies based on their specific goals or mission. While these missions are important to those they serve, they do not necessarily meet the needs of a common good. Take for example the Department of Justice, the Department of Homeland Security, and the Department of Education. Each of these agencies offers grants designed to serve the needs of states and local agencies. It is rare, however, that these agencies coordinate their efforts and require these funds to be used jointly or leveraged to serve a common good.

One of the final indignities regarding sustainability of programs is that if a program is effective, the funds are cut! Why would you not reward and promote programs that have been successful, thereby enabling the programs (with a requirement in future funding) to help other agencies or service providers, both public and private. Agencies invest time, energy, and limited funding into these programs. To not support the outcomes and take advantage of their successes is poor fiscal planning in my opinion.

Lastly, the sun-setting of grant funding creates an unmet need for newly created programs. In many programs, services are established or programs developed that then create service expectations in the local community. When the local entity cannot fiscally support these services due to grant money drying up, the program goes away leaving recipients empty handed and not served. Having the money to start up well meaning programs is great and serves to fill a short-term need. A more effective approach would be to tie grant funding to longer timelines for providing services and ensure that the written assurances of agencies supporting the grant application are, in fact, not just signatures but collaborative commitments. And by working with grant recipients in their local communities, rather than having them attend planning and training sessions in Washington, DC, you would go a long way to ensure the long term success of the programs.

Federal Direction and Support for Communications Systems

Currently, the various response agencies and those they support in Spokane have the following means of communications available for use in emergencies: "push to

talk" radios, such as Nextel®, UHF radios, VHF radios, 900 MHz radios, cellular phones, PDA's, Smart Phones, cell phones, laptop computers with a variety of communications software platforms, personal recreation radios, and PC-based Internet e-mail. As you can see, we are not lacking in the means of communicating; we are in fact buried in it.

Due to the number of divergent systems in place, we are less able today to communicate with other agencies and even within our own organizations. As an example, even the local branch of the U.S. Postal Service has its own internal PDA communications system. They have a wonderful means of communicating with their fellow members of the U.S. Postal Service, but it does not allow for communications with other agencies or those emergency responders who might be providing services to them.

The ability to communicate is essential in an emergency. From the advent of the NIMS system in the 1970s, the result of disastrous wildfires that occurred due in part to a lack of common communications systems, to the recent 9/11 tragedy in New York City where fire and police could not communicate, communication continues to be a critical issue. Common radio frequencies or communications methods are an important part of an essential communications system. Again, the breakdown of communication between first responders during Hurricane Katrina exemplifies this point.

Functional radio communication is one part of the solution, and human communication is another. Having agencies and end users meeting, planning, and training prior to an incident is critical to reducing response time and saving lives. Sitting down together and conducting pre-plan tactical exercises allows: 1) relationship building, 2) establishment of trust; 3) an understanding of the other agency's or business' needs during an emergency; and 4) the development of a common plan of action.

In Spokane, we use a crisis management program that facilitates collaborative pre-planning sessions and collection of critical data about key facilities. In addition to providing a common platform for data collection (including photos, organizational charts, floor plans, site plans, hazard chemical listings, etc.), it provides the necessary forum for the pre-incident planning. In my experience, this approach is critical in breaking down communication barriers and building trust between first responder agencies and the organizations they serve.

One of the benefits of the crisis management system developed by the State of Washington is that it is a statewide program. In Washington, all first responders, including police, fire, State Patrol, and others all have access to the same master database of information. The Washington Association of Sheriffs and Police Chiefs is responsible for the crisis management system, assuring that there is a common platform for data collection, training, procedures, response policies, and data security between local, county, and state first responders and their recipients.

If each local fire, police, and emergency management agency chose to use a different system, a coordinated response would be difficult.

Establishing a standardized statewide system is certainly not without its difficulties, especially those issues concerning "turf," budgets, and political concerns. But once agencies begin to use the system in actual emergencies, most of these issues resolve themselves and the agencies begin to see the inherent value of such a system. In our case, the CMS approach has truly served as a catalyst for collaboration and problem resolution. This type of program fosters communication, collaboration, and helps to build trusted relationships, all of which are critical factors during an actual emergency situation when lives and property are on the line.

Suggestions and Recommendations

1. *Facilitate relationship-building between agencies* at the local, state and national level, both within individual disciplines and between different types of agencies and organizations. Providing for training, in-services, and product conferences where planning, response, resolution and recovery conversations could be facilitated to establish common ground and exchange key information.

2. *Provide for sustainable funding of model programs* based on the requirement that agencies share their expertise and experience with others in their industry. The funding would be broad-based in that it would come from various agencies and serve to establish and maintain collaboration between local agencies and those they serve. It would encourage local investment of time, talent, and funding to create joint planning and response.

3. *Develop and adopt communication models* that can be implemented on a local or statewide basis. Support programs that facilitate pre-incident data collection and pre-plan tactical exercises, and encourage relationship-building between emergency responders and those they serve.

4. *Support the development of an "all hazards" approach* to emergencies, disasters and crises by providing all first responders with the basics in response protocols, communication, and incident response. Encourage adoption of NIMS / ICS protocols. Provide ICS training not only for police and fire services, but also for other emergency responders, including those in the public and private sector who will be responsible for ensuring their own employees' safety during the early stages of a crisis.

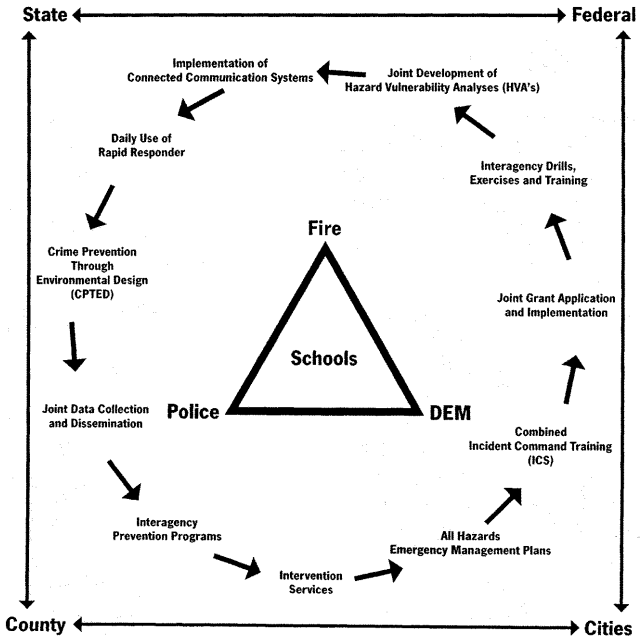
5. *Establish model plans for response to various emergencies, disasters and crises.* Select a lead federal agency in each area that would become the "go-to" agency. This would reduce competition between agencies, create efficiencies at the Federal level, and reduce confusion on the part of local agencies regarding direction.

Once again, I appreciate the opportunity to come before this subcommittee to share my views on these subjects.

I will be available for any questions.

Thank you.

A Collaborative Model for Providing Prevention, Intervention, Emergency Response and Recovery Services



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

I want to thank all the witnesses for their testimony. More than that, I would like to thank you for the work that you have already done in terms of responding to the various hazards, specifically terrorism, but all of the hazards that may affect your facilities wherever they might be.

I would like to ask one question to all four of you on the panel.

It seems to me that all four of you have talked about communications being extremely important, communications at the time of an incident, but even before that, communications in preparation for any type of problem, with local authorities, in some cases federal authorities.

My question is this: While the detail of information that you have, the digitalized documents that actually give people a blueprint and a visual of where they go and where vulnerabilities are, I presume you would be very concerned about that falling into the wrong hands. Has there been any concern expressed by any of you about this information getting public?

For instance, we do have the Freedom of Information Act. There are certain exceptions that we have built into the legislation that prohibit that from being turned over to the public.

But have any of you had that concern raised, and if you have raised it, have you had responses that are satisfactory to you by the authorities, either local, state or federal?

Mr. Millar?

Mr. MILLAR. Yes, we have had that concern. However, we do believe that the steps taken by the Congress a couple of years ago to change, give those exceptions, as you have said, have taken care of it. That has greatly enlarged our ability to share among transit properties. So I do not believe that is a significant problem to us right now.

Mr. LOWY. We are nervous about the issues there. Not only do we have the plans digitized and we give an update disk to local authorities each month, we also have then on the Internet. We have a Web site that is available where the local police, fire, ambulance, et cetera, have access to the mall that they may be dealing with.

The issue for us, though, is that since we deal with them on such a local level, I would be surprised if even as you get higher up in the LAPD or certain of the police departments that we deal with that even know that that actually happens. When we deal with them, we deal with the local watch commander or the person in the local patrol cars. We go as far as having to buy them actually laptop computers because they do not have them to access the information.

So while it is a risk, it is one that we deem appropriate because there is no other way to inform them and give them all the information they need.

Mr. LUNGREN. So you are not sure exactly who all has it within the departments that you are dealing with?

Mr. LOWY. We know who we are dealing with who has it. We do not know how far up the chain they actually send them and deal with the authorities. It also depends on how large a city you are dealing with or how small a city.

Mr. LUNGREN. Sure.

Mr. LOWY. In Los Angeles, such a large city, if it is not the West L.A. guys who know what we are dealing with, I would be surprised if they know what is going on downtown. That is no opinion about the city and how it is run. It is just such a large city.

Mr. LUNGREN. Just an observation?

Mr. LOWY. Yes, just an observation.

Mr. LUNGREN. Mr. Norton?

Mr. NORTON. We have taken steps post–9/11 with regards to this, especially in New York City, where a lot of our building documents were a matter of public record. Anybody could go down to city hall and pull these documents and do studies on them.

There was, working in conjunction with the Real Estate Board of New York, a law passed that there is a signature now required by the owner of that building if somebody goes down and is trying to get reference to that particular site. So that was a good thing that was implemented.

Additionally, in other markets where we used to have readily available, and I am speaking on behalf of commercial office buildings, plans for potential leasing and potential bringing in tenants, that kind of data is now secured both internally within the company and outside as well as off-site locations. So in the event of an emergency, we have access to that and we can get that to federal and local officials.

Again, I think it is important to emphasize we need to build the trust, and I think you have to earn that trust over time in working in conjunction with the federal, state and local.

We have done that in New York City and we feel that working with them and having them look at our high-profile assets, they have a very comfortable level of if there was an issue that came up, they understand what we are up against and they understand how to attack it, unlike the World Trade Center when they went down. There were no plans. They did now know where people were down in the retail. So there were a lot of lessons learned there.

Mr. LUNGREN. Mr. Madsen?

Mr. MADSEN. Three points.

The data-set that we have in Spokane and Washington state is controlled by the Washington Association of Sheriffs and Police Chiefs. They own that data as such, so it is confidential in that nature.

Secondarily, there are different levels of access in terms of us being able to authorize different agencies, whether it is police, fire, or the Department of Emergency Management.

And then the last point is really about the control of the data, while still allowing it to be used. We had a flood in one of our high schools. That data was very important to the maintenance department to save a $100,000 gym floor. If we regulate it down to a point where it can only be used for one purpose, I think that that is wasted financial dollars. Again, that all-hazards approach is very important. That data can be used for a multitude of different things and it would be a shame to waste it. It is secure. We can limit it, but it has a multitude of purposes.

Mr. LUNGREN. Thank you very much.

Mr. Pascrell is recognized for 5 minutes.

Mr. PASCRELL. Thank you, Mr. Chairman.

Mr. Madsen, I am very interested in what we tell kids about impending threats. I want to ask you a couple of questions, if you will respond, since you are there day to day.

How do you prepare children to respond to an attack without inducing fear in those kids? How do you do that?

Mr. MADSEN. We have, for the last 10 years, done training with our staff and our students. We have a four-step process. That process starts with the general orientation of the principal of the building to let them know about the district-wide plan, our three levels of crisis codes. From there, we then move on to the building staff itself.

The reason for that first and second step is to make sure that the building staff, the school staff, have an understanding that their principal, their person in charge of the building, has a level of understanding and they then in turn have a confidence with them.

We then move on to the third level, which is actually conducting tabletop exercises or small drills.

Mr. PASCRELL. What do you tell the kids before you are conducting the drills? Why are we conducting the drills? What are you telling these kids?

Mr. MADSEN. That is the fourth step, and that is publicizing to both parents in newsletters as well as students in orientation that we are going to be doing these drills, again from an all-hazards approach. It does not matter whether it is a terrorist activity, a school shooter, or a railroad tanker overturned by a school. We want to be prepared.

They do nine fire drills every year. We are very well supported by the superintendent. In addition to that, we do two crisis drills. Those are active drills that are done, both walk-down as well as all-hazard.

It is to the point where they are not fearful. It is commonplace, much like throughout this nation for 100 years we have done fire drills. It is the same level of preparedness, and just as they are not anxious because of the ongoing nine fire drills, their doing the two crisis drills every year allows them to not be anxious.

Mr. PASCRELL. So what you are telling us is that what you are telling children, communicating to children, is that we are stepping up the process, the mechanism, but really this is a fire drill we are doing which will encompass the entire school that you are in. Is that what you are telling kids?

Mr. MADSEN. It is moving beyond just a hazard of fire itself in a building, but all other hazards that could occur. Unfortunately in our nation, with what is occurring, we need to be prepared. We want to keep you safe. We tell parents we want to keep their children safe.

We have had very, very little push-back from parents in regard to that these live drills. We are doing them throughout the school district at all levels, elementary, middle and high school in 55 facilities.

Mr. PASCRELL. Spokane schools, I imagine, have quite a few police officers in them with regard to the COPS program, which was a very successful program. What experience have you had with the very police that are already in your schools?

Mr. MADSEN. There are two levels of police. We have our own Spokane public school district resource officers. There are 11 of them located throughout the elementary, middle and six particularly in the high schools. We did have six SROs as part of that COPS in-schools program.

Those funds have gone away, and so unfortunately we do not have the Spokane Police Department SRO program currently. We still have retained the 11 officers and I know that the chief has prioritized the SROs to come back first on his budget.

Mr. PASCRELL. Mr. Millar, if I may?

Mr. MILLAR. Yes, sir.

Mr. PASCRELL. In your testimony, you talked about not only the lack of response from Washington and this huge $6 billion inventory of needs that you laid out for us. And you are disappointed, correct me if I am wrong, at the $600 million response in the 2006 budget. Is that correct so far?

Mr. MILLAR. That is correct so far.

Mr. PASCRELL. Let me ask you this question. It seems that you spent some emphasis on how the money gets to the transit systems. You are recommending and suggesting, I think, a change in how this money is distributed, since a lot of it has never gotten to the point of implementation.

What you are suggesting is, are you not, the money go directly to the transit system, rather than go through the state administrative system. Would you explain that and why you believe that the system should change?

Mr. MILLAR. Yes, sir. Transit systems are responsible for the safety and security of their customers. We understand that. We have long-time direct relationships with the federal government, primarily through the Department of Transportation. We are used to applying for federal money. We are used to receiving it. We are used to all the requirements for audit and other things that necessarily come with the federal government. We do not believe that there is any value-added by sending it through the states. It is simply another step.

Now, we certainly agree that the states have statewide planning responsibilities, and we certainly agree that the money that we would receive ought to be consistent with the statewide plans, much the way transportation money is now distributed. It has to be consistent with area-wide and statewide plans. But we see no value in sending it through the states.

In addition, the Congress at least 2 years ago authorized as much as 20 percent of the money intended for transit to be skimmed off by the state. Now, last year the Appropriations Committee put a 3 percent limit on it, but still we do not see why 3 percent of the money that should be going to improve security for our customers, your constituents, ought to go off to some administrative red tape. It makes no sense, never mind the time delays and all the other aspects of it.

Mr. PASCRELL. Thank you for the response.

Mr. Chairman?

Mr. LUNGREN. Thank you.

The chair now recognizes Mr. Linder for 5 minutes.

Mr. LINDER. Mr. Millar, if $600 million is not enough, how much is enough?

Mr. MILLAR. Let's be clear about the $600 million. The president's proposal was to take several infrastructure groups, public transit, railroads, ports, a number of other group, and lump them all together to $600 million. So even on my happiest day, I could not imagine, even if the Congress appropriated $600 million, that public transit would get anything other than a small portion of that because the needs in the other areas are great as well.

What we have suggested is that we work with the Congress and the administration on about a $6 billion program. We could not spend all that money in a single year. We have suggested that it be spread over 3 years. We do believe that once this initial investment is made in capital infrastructure improvement, in training, in research, in planning, there will be an ongoing need, but it will be a much smaller need. It will be perhaps $800 million a year, something like that.

But we simply need to bring our systems up to standard; do common sense improvements. As the chairman has said and we completely agree, we are not talking about an airport-style screen every passenger, but we do believe the kinds of improvements that I have spoken about in my testimony, which everyone agrees need to be done, ought to be done. It is a partnership between the federal government, state government, local government, and we are prepared to be part of that partnership.

Mr. LINDER. Mr. Lowy, how many owners of real estate, organizations are doing this, digitizing their plans?

Mr. LOWY. As far as I understand, we are the only one that I know of. It is something we actually developed ourselves. As we were involved, we were in the retail facility at the World Trade Center prior to 9/11. It was something that we started doing even before that. Mainly the issue there is to be able in an emergency to know where all the entries and exists are; how to get people in and out; and how to get the first responders into the facilities.

Mr. LINDER. And that is in your interest?

Mr. LOWY. That is definitely in our interest, and in the interest of our customers.

Mr. LINDER. Mr. Norton, why aren't other organizations doing that?

Mr. NORTON. I cannot speak for what other organizations are doing with regard to digitizing. But as I stated earlier, we have taken precautions post–9/11 with regard to building plans, securing them, making sure in the event, especially on a high-profile asset like the ones that I had mentioned earlier, that we are prepared. If an event does take place, we are prepared to go in with both federal and local governments and assess that situation with the proper plans.

Again, I cannot speak for what the rest of the industry and what they are doing and why they are not doing it.

Mr. LINDER. Do you have a rough idea, Mr. Lowy, of how much you have spent doing this?

Mr. LOWY. Just on the digitization? What we have actually done is we have probably spent on the investment in security somewhere around $25 million a year on capital items, and about $40 million

a year on operations. But the digitization of the plans and what we have done, we have actually created our own internal systems that integrate the digitization of the plans, the CCTV cameras that we use and all of the information on the malls that we can use remotely are on-site, really in response to what happened to us at the World Trade Center.

Because we have been involved in it and have dealt with it, we have unfortunately a knowledge and an expertise that we would rather not have. But once we saw all the issues that we faced, we have just been developing these systems for the last 4 or 5 years in-house. The problem at the end of the day, though, is while we can do this for our facilities, integrated with all these other office buildings and all the other cities and everything, and we need to be part of the wider community as well.

Mr. LINDER. Mr. Norton, why isn't it in the interests of BOMA to spread this information and do it on your own?

Mr. NORTON. Again, I cannot speak for BOMA, but again for Tishman Speyer's properties, we, and I think there are organizations on the vendor side that have new programs out there that you can actually buy into, are looking at this. Again, are you going to do a suburban building in Phoenix versus a high-profile asset that sits over a transit station in midtown Manhattan? I think post–9/11 we have put a lot of emphasis on just gathering that data and making sure it is secure and safeguarded.

Again, I think it is something of the future, especially with the computer age, that we will continue to look at this and eventually get all of our buildings as an industry on this kind of a program. That will then be shared. Again, I think it will take getting more association with DHS and the other state and local government and federal agencies more time in getting comfortable with these organizations, to start sharing this kind of information. Because I think it would be overwhelming to try to get all this information and give it to these people.

In the commercial real estate sector, it changes. You will move tenants in; you will move them out. You will reconstruct space. You will add floors and take floors down. So it is a continually changing process.

So to update and keep plans accurate on such a mass volume of real estate throughout the portfolio of the United States that we are focusing on, I think would be a big undertaking. I think in time you will have to address it. It will have to be addressed.

Mr. LINDER. Thank you, Mr. Chairman.

Mr. LUNGREN. The gentleman, Mr. Dicks, is recognized for 5 minutes.

Mr. DICKS. Thank you very much.

I want to thank all the witnesses for their testimony, particularly Mr. Madsen. I want to welcome you here to the committee. I appreciate your work on the school mapping program.

The incident that occurred at Lewis and Clark High School, which you referred to in your testimony, was terrifying, but lives were very likely saved because of your mapping program that had just been implemented a couple of months before, which enabled first responders to see detailed maps and information about the high school while they were traveling to the scene. Instead of tak-

ing many precious minutes to formulate a response, once they got the high school police were able to hit the ground running.

That is the key to this mapping program, that you have all the information gathered and in a PC you can go through it as you proceed out to the incident, wherever it is.

Mr. MADSEN. You can access it in a variety of fashions. You can have it on the hard disk as I do on my laptop here. You can do it with a thumb-drive or you can do it via the Web. The benefit of the program is two-fold. One is the data-set itself. The other is the creation of trust and relationships. The pre-planning tactical sessions that were done prior to the incident between police, fire, transportation and the school district is one of the critical pieces.

Mr. DICKS. I would say to my colleagues on the committee, I am very proud of what Washington state has done on this. Washington has completed the emergency planning, mapping and inventorying all of the public high schools in the state, over 400. The state legislature has initiated funding for mapping of all public elementary and secondary schools. The year-long project to map the more than 1,275 elementary and middle schools began this July.

Also, we have done a program on critical infrastructure in the state of Washington so that key buildings, Washington has entered over 1,200 sites and 6,500 individual buildings into the critical infrastructure planning and incident management system, which I think will give first responders in our state a much better opportunity in a crisis to be able to deal with that particular facility. I think this technology, which has been developed by a company not in my district, but in Seattle, Prepared Response, Inc., they build and deploy this school mapping and solutions used by the state of Washington.

So I want to commend you for your work on this and your involvement and leadership in the Spokane area. You need a little leadership over there these days. But honestly, you guys have done a great job and we are proud of you.

Also on the question of transportation, I agree. I think we need to have a more even-handed approach to this thing. My view of it is a lot of the money has been spent on air transportation, and these other modes have not been given the consideration that they need to.

I also want to thank the witnesses from the private sector. I would recommend that you take a look at what we are doing out in the state of Washington. I think in major cities to have this kind of a mapping program where they really can look and have the analysis of these buildings ahead of time would help in any situation.

I thank you for my time, Mr. Chairman.

Mr. LUNGREN. I thank the gentleman.

Mr. Langevin is recognized for 5 minutes.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Gentlemen, I thank you all for your testimony this morning. It has been very enlightening and the committee appreciates it.

Mr. Madsen, let me begin with you, if I could. In your testimony, you describe a sophisticated technological system to provide building plans and predetermined emergency response scenarios for first responders. I am actually familiar with the technology. It is actu-

ally very impressive. As my colleague Mr. Dicks just mentioned, the Lewis and Clark shooting incident proved that the system can mobilize police, fire and school security to quickly respond to an emergency.

My question, if I could just delve in a little bit and talk about again the costs: I think you have mentioned that already, but the costs associated with implementing the system, and if I could ask how did your school district pay for the system? Did you receive any federal assistance in helping to pay for those costs?

And if you could just elaborate a little bit for the committee on what other soft targets could potentially benefit from a similar implementation.

Mr. MADSEN. Our funding in Spokane public schools has come from a variety of sources. The initial funding, by us being proactive and actually wanting to be part of a pilot, we do that quite a bit, allowed us to be part of the state pilot project, which allowed us to be mapping Lewis and Clark High School when that incident happened.

The rest of the high schools came from the state, funding through the state legislature. Our middle schools were a separate grant, privately funded. Our elementary schools, I attached that to our Safe Schools/Healthy Students Grant that we applied for last year and received this year.

Our school district, along with five others, share a $8.3 million, of which a portion of that, about $250,000, was assigned to our 35 elementary schools and the other 27 elementary and middle schools in the other school districts.

So it is creative financing. It runs anywhere from $5,000 to $12,000 per building. Then it is just time from there on maintaining that data.

Mr. LANGEVIN. And can you elaborate for the committee on other soft targets, buildings, assets, that could benefit from the technology?

Mr. MADSEN. Currently, we are working on our school buses. I feel—and I am in a very unique position with both safety, transportation and security departments, to see kind of a bigger picture.

I think that the issue with school buses in our nation, but specifically in Spokane, is critical. We will have all of our school buses, the six different types that we operate, with our contractor, Laidlaw as a partner, actually mapped. So all of the exits, all of the electrical shutoffs, the fuel tanks, all of those types of systems or components in regard to the physical school bus.

So whether it is a rollover or whether it is a terrorist or hostage situation or a fire on board a bus, fire and police, school security and transportation all have access to that critical data. That is my next step in our school district, is to map the actual school buses. It is not a building, but it is a rolling facility for us, and it has up to 72 students.

Mr. LANGEVIN. Thank you.

Mr. DICKS. Would my colleague yield just for a quick point?

Mr. LANGEVIN. Of course.

Mr. DICKS. RPI, the company, has mapped all types of venues, including schools, hospitals, port facilities, commercial office build-

ings, water treatment facilities, and Navy ships. So this has been used broadly in many different contexts.

I appreciate your yielding.

Mr. LANGEVIN. Thank you. I appreciate your making that point.

Quickly before my time runs out, to Mr. Lowy. Your testimony indicates that your company spends about 20 percent of your operating costs on security.

Can you just tell us, is this amount standard across the commercial real estate industry? At what point, I should say is there a point, where the economic costs of security have a greater affect on your bottom line where the cost-benefit analysis shifts?

Mr. LOWY. I think the issue is not how much money we spend, but how effective is the money that we spend. Security is now the single largest line item in the mall industry itself, the single largest cost line item that we face, which is even more than our cleaning costs, which cleaning used to be major item.

Where it is really affecting it is in the mall industry you tend to be able to collect the cost of managing and operating a mall back from the merchants. So what happens is at the end of the day the cost of security ends up in the price of goods that are sold to the consumer. It is in essence added to the rent that a retailer pays.

The issue with those costs, though, is a retailer can only pay a certain percentage of the cost of these total sales at the end of the day. The cost of security, that is increasing substantially after 9/11, while it is not eating into the bottom line just now, it all depends on how much you can pass on to the consumer or not, what happens with general prices, and then what happens with the total cost of operations for a retailer.

I would like to add to the last testimony, just for one second.

We actually do something similar to what they are doing in Washington in our malls across the country. We are actually have integrated that into our CCTV cameras, which is also on the Internet. We run a 24-hour-a-day central facility which we can access and also local authorities can access, which has all the plans, all the maps, all the fire hydrants, everything available to them, as well as real-time online cameras that we use for management as well.

So we have actually implemented that in the mall business here in the U.S. and we are actually exporting that to the U.K. within our own portfolio.

Mr. LANGEVIN. I see my time has expired. Thank you all for your testimony and for being here. It has been very helpful. Thank you.

Mr. LUNGREN. The chair would state that we have received a statement of testimony from the International Council of Shopping Centers, who have requested that it be entered into the record. If there is no objection, I will do so.

So ordered.

FOR THE RECORD

STATEMENT PREPARED ON BEHALF OF THE INTERNATIONAL COUNCIL OF SHOPPING CENTERS

SEPTEMBER 7, 2005

Founded in 1957, the International Council of Shopping Centers (ICSC) is the premier global trade and professional association of the retail real estate industry. Its more than 50,000 members in 96 countries include shopping center owners, developers, managers, marketing specialists, investors, retailers and brokers, as well as academics and public officials. As a global trade association, ICSC has relationships with 25 national and regional shopping center councils throughout the world.

The shopping center industry takes its role of providing a safe and comfortable environment in which to shop very seriously. Security has always been a priority of the industry. Simply put, consumers will not shop at a shopping center that they do not feel is safe.

Shopping centers employ well-trained professional security officers and enjoy excellent working relationships with their local municipal police departments. In fact, many shopping centers actually have a police sub-station located within the center. Those that do not have a police sub-station are frequently visited by local police patrols. While the shopping center industry has a long history of providing a safe environment in which to shop, we recognized that the terrorist attacks on our nation forever altered the way we police and secure our shopping centers.

In October 2001, ICSC and the shopping center industry convened a conference call with the newly formed Department of Homeland Security (DHS) and representatives of the Federal Bureau of Investigation (FBI). The conference call was initiated by ICSC to establish a working relationship with DHS and to allow shopping center security professionals and law enforcement officials the opportunity to share security practices and procedures. In all, over 1,000 shopping center industry professionals participated in the call. Since that initial call, ICSC has been in constant contact with DHS and the FBI to provide a communication channel for our members.

Communication is paramount. ICSC joined with other real estate associations in creating an Information Sharing and Analysis Center (ISAC) to expedite two-way security intelligence between retail properties and DHS. ICSC will continue to monitor the threat level and communicate to our members any and all information from government authorities as soon as it becomes available.

ICSC members have actively participated in the DHS Basic Terrorism Awareness Training program. In the first year, ICSC had 609 participants representing 20 programs. In 2005, 18 programs were involved with over 500 participants. In addition, ICSC is developing a comprehensive training program that addresses the potential for chemical, biological or radiological terrorism. Designed to meet the DHS Office of Domestic Preparedness requirements for the first-responder community, ICSC's program is utilizing a "train-the-trainer" approach. Each participant will be expected to share the program's training insights with other security personnel thereby enabling the industry to maximize the effectiveness of the program.

Since September 11, 2001, the shopping center industry has been on a heightened state of alert. Many of the security procedures the industry implemented will be obvious to consumers. These include but are not limited to:

- Increased patrols by uniformed security personnel in and outside of the shopping center.
- Increased patrols by uniformed local police officers in and outside of the shopping center.
- No overnight parking in parking lots.
- No curbside parking.
- The use of barriers and or blockades in front of entrances.
- The use of security surveillance camera systems.

In addition to these security procedures, the shopping center industry has implemented many programs and policies that go on "behind the scenes" and will not be obvious to consumers. These include but are not limited to:

- The lockdown of heating and ventilation systems with access limited to center personnel.
- The lockdown of loading docks.
- The lockdown of supply corridors.
- Searches of incoming deliveries.
- Background investigations of center personnel.

- All workmen entering a center must be prescreened, have identification, and report to security before starting work.
- Increased patrols by non-uniformed security personnel.
- Increased patrols by non-uniformed local police officers.

Shopping center security is very *site-specific.* What is needed and used at one center may not be appropriate at another center. There are many factors that are used by shopping center security professionals in concert with their local police departments to determine the level of security required. These factors include but are not limited to the size of the center, location of the center, history of criminal activity in the surrounding community, and size of the local police department.

While we are under a heightened state of alert, some centers may choose to change or increase their level of security. Others may not because they are confident the level of security in place is sufficient. Again, security is a *site-specific* science and it is important for consumers to have a sense of normalcy in their lives, and that includes the ability to travel freely about our shopping centers without being unduly inconvenienced.

As Peter Lowy of The Westfield Group demonstrated in his testimony before this subcommittee, the retail real estate community is actively engaged in responding to the lessons of September 11 as well as the attacks in London. ICSC appreciates this opportunity to provide the subcommittee with an additional perspective of the overall shopping center industry. Please do not hesitate to call upon ICSC or its individual members during your future deliberations.

Mr. LUNGREN. The Gentlelady from Texas?

Ms. JACKSON-LEE. Thank you very much, Mr. Chairman.

The issue before us is an extremely important issue and I will pose a question based upon your expertise. I would like to acknowledge the committee for its wisdom in delaying the other witnesses who are presently dealing with a horrific horror in our own nation that is occurring.

In light of that and in light of my representation of the impact area in Houston, I just want to make these remarks for the committee's consideration, and as well for the record. It is very important that the work of rescue and recovery dealing with Hurricane Katrina continues, so I am the least willing to distract individuals from the work at hand. But I do believe that there should be important interaction.

I note that a number of impacted members are on the Homeland Security Committee and are probably functioning from one place to another trying to assist their constituents and others. But I do believe, Mr. Chairman, and to the prospective full committee chairman and ranking member, that we should be having daily briefings either by conference call or otherwise of the progress that is being made in the region.

I think there are some serious policy issues that should be addressed as well, particularly on the question of the human devastation. The individuals, in essence, in Houston for example, probably the largest repository at this time, placement of evacuee survivors, has an array of disparate policies that are enormously confusing, particularly with the presence or the work of the Red Cross and FEMA and the need for there to be some alignment and cooperation. The establishment of Red Cross sites is not really organized. The presence of FEMA personnel is not there yet, not enough. The need for increased technology, a system-wide technology that would be able to reunite families.

And then one of such magnitude that I think that we need an immediate cease-secession order, cease and desist. And that is the random evacuation of persons who desire not to be evacuated to places unknown. There are policies of putting people on airplanes,

and when the door is open in the jurisdiction they say, "They put me on the plane, they closed the door, and I didn't even know where I was going." And this is in America.

So I hope that, although Mr. Chertoff is certainly consumed with the responsibilities, I think part of the problem was that he was consumed and not in communication. Many members cited that on the floor of the House and I think that is unpardonable without excuse, inexcusable, if you will, and unacceptable. It certainly is unacceptable for those of us who have a large share of the responsibility, willingly so.

I cannot announce for you, if you will, or articulate for you the wide depth of charitable expression in Houston; $10 million that the city voted on in an emergency session just on Monday; feeding, if you will, food service bills for a day-and-a-half of $225,000 at one site; individuals who have opened homes and gyms and otherwise taken money out of their own pocket; others who are in hotels; 15,000 Vietnamese are in our community that we have to address through their language; a number of people from Central America.

And there are no enunciated policy positions dealing with this vast number of people except waving them out across America against their will. It is well known that the leaders, the elected persons of Louisiana want their constituents to return home.

So we have a crisis that we need to deal with here. I expect and would hope that this committee would have immediate hearings or briefings. If they can be abbreviated, so be it, but we cannot operate in the dark again.

I thank the committee for its indulgence.

Gentlemen, your issue is very important, but I am facing day-to-day life and death situations, as my colleagues in Louisiana and Mississippi are. I have the aftermath. They have the real impact. I believe this is something egregious occurring and I believe we should act immediately.

Mr. LUNGREN. I thank the Gentlelady for her comments.

Mr. Souder is recognized for 5 minutes.

Mr. SOUDER. Thank you.

I apologize that I missed the first panel and the testimony. I have been trying to go through the testimony here. I had actually a hearing that I had to start in my own subcommittee, as well as another meeting.

I have become particularly interested in this, having gone over with Curt Weldon over to London. We met with Prime Minister Blair shortly thereafter and gave him our congressional condolences, and was there particularly on the day where they had just had the shooting of the suspect who defied the authorities, and they thought potentially had a bomb.

I wondered, Mr. Millar, do security guards have the ability to detain people, and if they restrain, can they shoot at them? Do you have the legal authority if they make a judgment on the ground that many people may die if they do not act, can they act?

Mr. MILLAR. The individual police powers that individual transit police forces have is generally speaking governed by the state law of that particular state.

So, for example, I used to run a transit system in Pennsylvania. Our police officers had full police powers and were trained and li-

censed to carry guns. Obviously, that was the absolute last resort, but in that case they were trained to use their judgment and were permitted to use guns if appropriate.

So it depends on the state and depends on the jurisdiction as to what the law allows and what the orders are that guide what the officers do.

Mr. SOUDER. In going through your testimony and looking at this problem in general, we spent so much time on airports and the numbers that use mass transit every day are much harder to screen and go through.

Mr. MILLAR. Yes, sir.

Mr. SOUDER. Yet much of what we seem to be oriented toward video surveillance and so on, seem to be more how to find the perpetrator after they have blown us up.

Do you believe that it is possible to do more if we get a network, a security pass system that works for airports, that that can also be used long-term for mass transit, particularly for subways, but also for buses and other things?

Or is this just not going to be possible because of the scale? When you think of the Staten Island Ferry and the numbers there, and people coming in at the last minute and holding the doors open, I mean, is this even conceivable?

Mr. MILLAR. We do not believe that with current technology it is practical to screen every person who would choose to use the public transit systems. There are thousands and thousands of railroad stations. There are tens of thousands of bus stops. You are talking about more than 100,000 vehicles that provide service across the country, from the very largest cities to the very small.

We believe that there are other steps that must be taken. We believe you need to start with good intelligence. In my testimony, I emphasize the fact that I think we need to continue the ISAC, the Information Sharing Analysis Center for Public Transportation, for example.

We believe that you need to secure the facilities the best you can. Some of that is very low-tech and some is very high-tech. It is low-tech in the sense of having better fending around garages where trains and buses are stored. It is high-tech in the sense of in-stations have biological sensors, chemical sensors, radiological sensors.

We believe that surveillance cameras have a very important role to play. We believe that the experience in London showed that. For example, while the terrible tragedy that occurred in London, we know over the last several years the camera system there has prevented at least 20 major attacks on the system. We know that in the aftermath of the attack, the camera system in London has been instrumental in obtaining evidence and ultimately obtaining the arrest of the perpetrators.

So there are several different steps that must be taken, in our view. We believe these steps are common sense steps. We are not asking for pie-in-the-sky things that do not make sense, but it does require an additional investment, as my testimony lays out.

Mr. SOUDER. With the chairman's indulgence, I would like to ask a question of Mr. Madsen that also may apply to those who work with the malls.

At Columbine High School and the aftermath, over in the Education Committee one thing we learned, part of the reason for the delay is the police went in and the cafeteria had been remodeled. The map that they had did not work, and they had to come out, and a student and a teacher had to draw how the doors were shaped.

A similar thing in 9/11, apparently going into the World Trade Center, some of the stairways were in different places because often when a school is redone, when a mall is redone, the plans that they find do not have the updates on them for the emergency personnel.

Is this something that your school system has addressed? Is this something malls are addressing?

I know that it is happening across the country. It can be fairly expensive, but it is unbelievable that when we go into the buildings we do not know where the doors or the stairwells and so on are. It is kind of a basic thing we ought to be focusing on.

Mr. MADSEN. The system that we have allows us to update and uplink information, and then that is automatically downlinked to all of the other computers that store that data that police, fire, school district security access.

I have charged each of my district resource officers that responsibility to at least annually ensure that if there are any changes from a capital project standpoint that they communicate with our facilities department, get updated CAD drawings, and those are then entered into the system, much the same as organizational charts, photos from our photo ID system.

Individual district resource officers have buildings assigned to them, and that is one of their charges to ensure that that data is correct and updated on an annual basis.

Mr. SOUDER. Are the malls doing that as well? Obviously, if there are hostages; if there is a bomb in a location and our maps do not work, we are helpless.

Mr. LOWY. It is a little easier for us because we get to control the resources, rather than a city itself. With merchants coming in a changing in the mall all the time, we actually update them every month, and then we uplink them onto our Web site and then we send a new disk to the local police and fire every month. They are on mall properties all the time anyway so we have terrific relationships with them.

But you are right, if you do not update it every month or every year, the plans that you pull down can be old and things change.

The one issue about digitizing all of the plans and having first responders come and go is the initial costs may be high, but you have to also keep the ongoing expenditure because you must update them all the time, otherwise it is a waste of time.

Mr. SOUDER. Thank you.

Mr. LUNGREN. Mr. Lowy, you mentioned in your written testimony that—and I know it is not the total focus of this hearing, but it seems to me it is an important component in this whole process, and that is the extension of Terrorism Risk Insurance Act (TRIA). Why do you find that important enough to have mentioned it?

Mr. LOWY. It is a very important issue for us.

One of the issues we talked about a little bit is the amount of money we spend on security and why have we put all these systems in place. One of the issues that we face even with TRIA or without TRIA is it is very difficult for us to get terrorism insurance. So that the risk of insurance or the risk of a terrorism attack prior to 9/11 was actually taken by the insurance industry itself.

Without TRIA, we could not get enough insurance or in some cases any insurance for a terrorist attack, so the economic risk of that attack was moved over to the shareholders or the business owners or whoever else was earning the asset itself.

So one of the reasons we spend so much money and time on the security is that we are actually at risk, whether TRIA is in place or not right now. We cannot get enough coverage. We have $14 billion worth of assets in the U.S. We can get $800 million of coverage today. We believe that without TRIA being renewed, that coverage will fall to somewhere close to zero, and that we just will not have any ability to get insurance.

The issue with that, then, is if you get another attack similar to what went on with 9/11, we believe at the end of the day that the federal government will have to decide whether it will come back in and make all the losses, make everybody good and settle up all the losses for the people and/or the property. Or it will stay out and the economics effects on the economy will be much greater than happened in 9/11.

Just one last thing. The key in 9/11 to the economy being stable straight after the attack was that the federal government stepped up and put almost $30 billion into the economy to make good the losses and the victim's compensation fund.

Mr. LUNGREN. Even though TRIA is not under the jurisdiction of this committee, I happen to think it is important for us to look at because it is part of the total picture as we deal with the soft targets that are out there in private industry.

That leads me to another question. I would like to direct it to Mr. Lowy and Mr. Norton.

That is this. Mr. Lowy, you have talked about the specific way you have developed you own program digitalizing plans and so forth, making them available, updating them every 30 days. It is obviously not the standard in the industry right now. Some may say you are the leaders in the industry.

One of the concerns I have is this. How do we work from a governmental standpoint, working with those of you in the private sector, to emphasize best business practices that are actually best business practices?

That is, if some take certain steps that they can afford to take to protect them against or their assets against possible terrorist attack, does that leave others open to lawsuits thereafter such that you are fearful of exchanging information, or such that the business community is worried about establishing what the business practices are?

The reason why I say this is when we originally—I was outside the Congress at the time, but working on it—when TRIA was originally passed by the House, it contained in it some liability limitations with respect to terrorist attacks. When it went over to the Senate side, that was taken out.

The Administration, having looked at TRIA, is not quite as negative about it as I feared the Treasury Department would be, but they indicated that Congress needs to look at some changes in the program.

From your standpoint, both of you, is there a concern about liability after the fact that in some ways impedes the ability of your industry to get together and say, these are best business practices, or publish what the best business practices are, for fear that later on you will be subject to suits because you did not expend 20 percent of your capital as others have done?

Mr. LOWY. I think the way we look at it is if there is a terrorist incident, we are convinced we will be sued no matter what we do. Part of the issue in the testimony is that one of the things we are looking for from Homeland Security is that we might have best practices or the money we spend may be wasted. I doubt it is wasted, but we think we have best practices. But depending on the alert level that Homeland Security puts out depends on how we operate our malls.

I actually brought with me, which we would not put into the public record because it is a security document, what happens when the threat levels actually increase; what we actually do in the mall; how much more manpower; where do we put them; what do we do.

So we respond to Homeland Security, but we do not know if we respond in a manner that is in line with what the government thinks or not.

So at the end of the day, while it was not in my testimony, we would be looking for some form of safe harbor; that if there were best practices that came out from Homeland Security after a survey of what everybody does, that if we follow those practices we do get some safe harbor provision.

Mr. LUNGREN. My concern is at some point in time you could make us so hardened to attack that you cannot do your job. We could make every mall in America and every hotel in America and every business in America and every school in America basically impenetrable, but people would not want to go. People do not want to go to a moat. You do not want to go to a prison to enjoy your honeymoon. You know what I am saying.

Mr. LOWY. I agree.

Mr. LUNGREN. So how do we strike that balance and how do we in the Congress encourage such activity? TRIA is part of it, but best business practices are others. Maybe tax incentives are others. But how do we do it in a mix of incentives and disincentives such that we do respond to the terrorist attack, but we do not change essentially who and what we are?

Mr. LOWY. We agree with that. The biggest issue that we face is, while we all talk about security here, that is not my main focus in life, but we do have to make sure that our customers and our consumers are protected to the best of our ability, while keeping the malls open and while having freedom of movement, freedom of goods. At the end of the day, people have to come and shop and work within the society.

The way we look at it is in conjunction with TRIA. At the moment, we get no benefit on our insurance premiums for any of the security work that we do, any of these systems that we have de-

signed or any of the capital that we put in. Our insurance premiums are exactly the same as the person next door or the guy down the street.

We would hope that Congress could work with the insurance industry and ourselves; that if a certain set of practices were used, that we could then get some break on the insurance premiums that we are paying for terrorism insurance, because we are making our responses better, our targets better. At the end of the day, we are not looking to make our malls impenetrable because we actually need to operate in a capitalist society, which we honestly prefer to do.

Mr. DICKS. Mr. Chairman?

Mr. LUNGREN. Yes.

Mr. DICKS. Just for a second.

I think it is especially relevant on transportation what you just said. I mean, you are talking about malls, but you have to have transportation systems that the people can use in a timely way.

We have, for example, ferry systems in Washington state. If we had an inspection of every car or every truck, that would stop it. You would not be able to use the ferry system or the subway system. I think it is very relevant to the other witnesses here as well.

Mr. LUNGREN. Thank you.

I understand the Gentlelady has a statement to make?

Ms. JACKSON-LEE. Thank you very much, Mr. Chairman.

Gentlemen, the hearing is very important. I am going to ask unanimous consent to have my statement placed in the record, and subsequently pose questions dealing with best practices.

But as you realize, there are conflicting and competing concerns, and I want to thank you for this hearing and look forward to a further hearing.

Mr. LUNGREN. Without objection, so ordered.

The Gentleman from Indiana?

Mr. SOUDER. I wanted to make an additional comment. As a member of Congress, we all have different things in our district that shed light upon the different things. By the time we retire, we are almost up to where we understand.

This insurance question is huge, because it is not the insurance companies, it is the reinsurance companies. Lincoln Financial in Fort Wayne sold their big division to Swiss Re, and Swiss Re took a hit on 9/11 that was unbelievable because they had like 50 percent or 60 percent of all the reinsurance for the insurance companies.

The insurance companies do not hold the bag; they just hold a percent. They pass it off. American Specialty in my district handles a high percentage of stadiums, NASCAR places, amusement parks and so on, and they put together the packages. Right after 9/11, we sat down with the risk assessment people.

I mean, it is a tough decision right now whether to insure all you guys with their private capital, because unless we have these government programs to back it up, there is no way to factor in the risk of a failure without just assuming you are going to go bankrupt, then you do not have insurance anyway. Because if your reinsurance and your insurance preparers go bankrupt, the govern-

ment is doing to wind up, either the people are out or the government is there.

We have to have some form of backup supplemental. It is more of a question of what it is going to be and how much is going to be absorbed directly through the consumers; how much is going to be absorbed through taxes; and how much is going to be theoretically, businesses are just pass-through institutions.

It is a huge challenge because from the insurer's perspective, they do not know how to factor this risk either.

Mr. LOWY. As an industry, what we are really asking for is that the federal government give the reinsurance industry capacity so we can actually buy insurance at a reasonable cost. We are not looking for any handouts. We do not want this to be a big handout to the insurance industry. What we really need them to do is insure our risk at a reasonable cost for us to be able to deal with it.

Mr. SOUDER. What the chairman was saying in sharing best practices and risk pooling, while it may be counter to some things that we have looked at in the past, the fact is it is one of the only ways to keep the insurance rates in a reasonable way either to the taxpayers or to the consumers who are going to pay it in raised prices, because businesses, like you say, are going to pass it on. You are just a pass-through institution. You either have to reduce the quality of your products or the labor costs or something, or raise the prices.

This is a crux of how we are going to protect people, because if they cannot get insurance, we are in real trouble.

Mr. LOWY. The biggest fear we have without TRIA is there will not be terrorism insurance and the economy will actually be taking the risk, not the insurance industry.

Mr. LUNGREN. I thank the Gentleman from Indiana. Having been at Heinz Field in Pittsburgh this weekend to watch Notre Dame beat Pittsburgh, I compliment you on your dress today.

[Laughter.]

I will not say anything about the Washington Huskies.

I thank the witnesses for their valuable testimony and the members for their questions.

The members of the committee may have some additional questions for the witnesses, and we will ask you to respond to these in writing please. The hearing record will be held open for 10 days.

Let me once again thank you. Your very, very helpful testimony will assist us as we move forward.

Without objection, the committee stands adjourned.

[Whereupon, at 11:43 a.m., the subcommittee was adjourned.]

THE LONDON BOMBINGS: PROTECTING CIVILIAN TARGETS FROM TERRORIST ATTACKS PART II

Thursday, October 20, 2005

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON ECONOMIC SECURITY,
INFRASTRUCTURE PROTECTION, AND CYBERSECURITY,
Washington, DC.

The subcommittee met, pursuant to call, at 3:06 p.m., in Room 311, Cannon House Office Building, Hon. Dan Lungren [chairman of the subcommittee] presiding.

Present: Representatives Lungren, Pearce and Thompson (ex officio).

Mr. LUNGREN. The hearing of the Committee on Homeland Security, Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity will come to order.

The subcommittee is meeting today to hear testimony from the Department of Homeland Security on protecting soft targets from terrorist attacks.

I want to thank our panel of witnesses for joining us today. What we are doing today is convening as a continuation of a hearing that was held in the beginning of September on efforts to better secure our Nation's numerous soft targets. At that time we heard from representatives of shopping malls, office buildings and schools on their efforts to prepare for, protect against and mitigate a terrorist attack.

We originally planned on having a government panel before the private panel, but due to Hurricane Katrina and the workload that ensued afterwards, our DHS witnesses had to postpone until today. This was fortuitous in some respects as we were able to learn a lot from that first panel of witnesses, and we can now get some answers and clarification from the Department with respect to some of the issues that were raised at that time.

What became apparent during our first panel discussion on the soft target issue, and really an issue that we have grappled with time and time again on this committee, is how do we take our limited resources and expect to protect against an almost infinite number of civilian targets and terrorist scenarios. The response that we have collectively heard again and again to this problem is that our Nation must be risk-based in our approach to security.

I think it is important that we take time to realize what this would actually look like in practice and begin to think about how the Department can move forward towards utilizing this methodology across the board. In practice, a risk-based methodology means not focusing on each sector from top to bottom—it means not focusing on one sector at the expense of others. I don't expect the Department to secure, or for that matter, even to analyze, the risk of every single chemical facility in this country and then move on to do the same for dams and office buildings, and then off to malls and so forth. There are not enough resources to do this, and certainly not enough time. We must be acting as if the next terrorist attack is just around the corner. And, the job at the Department of Homeland Security, I believe, is to focus on securing the highest-risk sites first.

Each sector is filled with a mix of low, medium, and high-risk sites, the majority falling into the first two categories of medium to low risk. For every low risk site the Department spends time analyzing or securing in one sector, there is the potential for a high-risk site in another sector to go unaddressed—at least for a time. What we need is cross-sector risk analysis to identify the highest-priority sites across the country and across all sectors, and simultaneously be working to identify protective measures that can be taken to mitigate those risks. At the same time, we should be working with our partners in the private sector to develop guidance for the low and medium risk sites so they can improve the security practices there as well.

As Secretary Chertoff has said repeatedly since taking office earlier this year, Homeland Security must be more than simply reacting to the latest action of our adversary. We should avoid being dictated to by the "target du jour". We should be securing our homeland in a systematic and prioritized manner based on our best understanding of the risk.

When we originally scheduled this hearing, I was expecting that Members would focus on transit security in the wake of the London subway attacks. We now know from the President himself that we have foiled al-Qa'ida attacks aimed at apartment buildings, other urban targets, tourist sites and ships. And, of course, post-Katrina there is a renewed focus on the vulnerabilities of dams and levees. Yet we recently learned that the New Orleans levee system, which for years has been identified as being vulnerable to hurricanes with catastrophic consequences by DHS itself, was something that received little attention by either DHS or state officials prior to Katrina, even though a terrorist attack on the levee system could have been even more catastrophic than a hurricane. In fact, it is my information that this levee system was not even included on the Department's list of top priority assets, even though other less consequential sites did make that list because they fell within a particular sector. I would hope that we would be better—we have to be better about developing a truly prioritized national list and doing so quickly.

What I hope to hear from our witnesses today is how you are prioritizing across sectors, and what you are doing in real time to secure our most critical and most at risk infrastructure, whether

they be dams, levees, chemical plants, subways, apartment buildings, malls, you name it.

I thank the witnesses for their appearances today, and I recognize the Chairman of—excuse me, the Ranking Member—I keep calling him Chairman, I keep trying to get him to become a Republican.

PREPARED STATEMENT OF THE HON. DAN LUNGREN

OCTOBER 20, 2005

Good Afternoon everyone and I want to thank our panel of witnesses for joining us today. The Subcommittee is convening today as a continuation of a hearing that was held in the beginning of September on efforts to better secure our Nation's numerous soft targets. At that time, we heard from representatives of shopping malls, office buildings, and schools on their efforts to prepare for, protect against, and mitigate a terrorist attack.

We had originally planned on having the Government panel before the private panel, but due to Hurricane Katrina and the workload that ensued afterwards our DHS witnesses had to postpone until today. This was fortuitous in some respect, as we were able to learn a lot from that first panel of witnesses and we can now get some answers and clarification from the Department with respect to some of the issues that were raised then.

What became apparent during our first panel discussion of the soft target issue—and really, an issue that we have grappled with time and again on this Committee—is how do we take our limited resources and expect to protect against an almost infinite number of civilian targets and terrorist scenarios?

The response that we have collectively heard again and again to this problem is that the Nation must be "risk-based" in our approach to security. I think it?s important that we take time to realize what this would actually look like in practice and begin to think about how the Department can move towards utilizing this methodology across the board.

In practice, a risk-based methodology means not focusing on each sector from top to bottom—it means not focusing on one sector at the expense of others. I don't expect the Department to secure—or, for that matter, even to analyze the risk of—every single chemical facility in this country, and then move on to doing the same for dams, and then to office buildings, or to malls.

There are not enough resources to do this—and certainly not enough time. We must be acting as if the next terrorist attack is just around the corner. And your job, as the Department of Homeland Security, is to focus on securing +the highest risk sites first.

Each sector is filled with a mix of low, medium and high-risk sites—the majority falling within the first two categories of medium to low risk. And for every low-risk site that the Department spends time analyzing or securing in one sector, there is the potential for a high-risk site in another sector to go unaddressed.

What we need is cross-sector risk analysis to identify the highest priority sites across the country—**across all sectors**—and *simultaneously* be working to identify protective measures that can be taken to mitigate those risks. At the same time, we should be working with our partners in the private sector to develop guidance for the low and medium-risk sites so they can improve their security practices as well.

As Secretary Chertoff has said repeatedly since taking office earlier this year, homeland security must be more than simply reacting to the latest action of our adversary. We should be securing our homeland in a systematic and prioritized manner, based on our best understanding of the risk.

When we originally scheduled this hearing, I expected that Members would focus on transit security in the wake of the London subway attacks. We now know, from the President himself, that we have foiled al-Qa'ida attacks aimed at apartment buildings, other urban targets, tourist sites, and ships. And, of course, post-Katrina, there is a renewed focus on the vulnerabilities of dams and levees.

Yet we recently learned that the New Orleans levee system—which for years had been identified as being vulnerable to hurricanes with catastrophic consequences *by DHS itself*—was something that received little attention by either DHS or State officials prior to Katrina, even though a terrorist attack on the levee system could have been even more catastrophic than a hurricane. In fact, this levee system was not even included on the Department's list of top priority assets, even though other less consequential sites did make that list simply because they fell within a particular

sector. We have to be better about developing a truly prioritized, national list, and doing so quickly.

What I hope to hear from our witnesses today is how you are prioritizing *across* sectors, and what you are doing, in real time, to secure our most *critical* and most *at-risk* infrastructure—whether they are dams, levees, chemical plants, subways, or apartment buildings.

I thank the witnesses for their appearance today, and I will now recognize the Ranking Member, Ms. Sanchez, for any opening statement she may wish to make.

Mr. THOMPSON. You are already looking into the future.

Mr. LUNGREN. Well, maybe I am looking into the future. We would always welcome you in the Republican Party. The Chair now recognizes the Ranking Member of the full Committee, the gentleman from Mississippi, Mr. Thompson, for any statement he might have.

Mr. THOMPSON. Thank you very much, Mr. Chairman. The good thing about this committee is, as you know, whether you are Democrat or Republican, our real goal is to make sure that we are safe, and I can say that all our members see that as number one priority.

Let me welcome the panelists for today. Generally speaking, this would be a full panel, but when the Congressional schedule changes, people go to their districts real quick, and we understand that. I think their absence is no indication of them not being interested in this issue.

Like all Americans, I was shocked and repulsed by the terrorist attacks in London. This attack has served as a reminder that America and its close allies continue to face a determined enemy that thinks nothing of slaughtering innocent people.

I was troubled, I have to say, by Mr. Chertoff's comments yesterday before the Katrina Committee that he had to get his house in order. How many disasters, attacks, and close calls is it going to take before the Department of Homeland Security wakes up? First, we saw the Government's response to the hurricanes. Then we saw the disconnect between the Federal Government and the New York officials about threats to the city's subway systems. Two days ago the Baltimore tunnel was closed. I heard, as the tunnel closed, conflicting reports about whether it was a real or fake threat.

Mr. Chertoff, in your absence, while you have been putting your house in order, it has crumbled to the ground from neglect to its foundation and walls. Trust is important. I, along with every other American person, must be able to trust the Department of Homeland Security to perform at 100 percent, if not more. I am close to losing all trust.

With regard to our mass transit and passenger rail systems, I am especially worried. Almost 4 years after the September 11th terrorist attacks, passenger rail and transit security remains a Department of Homeland Security afterthought. While the United States has spent over 18 billion on aviation security since 9/11, we managed only to offer up 717 million for transit security. That simply falls too short, especially when one considers that every American takes mass transit 16 times more often than they travel by air.

The National Strategy for Transportation Security that the Department recently submitted that was supposed to lay the ground-

work for securing our mass transit systems was lacking. Indeed, it did not meet Congressionally mandated requirements.

Speaking of which, I want to know when DHS will start using the National Response Plan. Secretary Chertoff told Members of Congress yesterday that the Department did not have an integrated plan in place when Katrina struck. What about the National Response Plan? Did he forget about it? Is it another document that contractors put together that wastes taxpayers' dollars because the Department doesn't think it is good? I would like to know.

One thing I would also like to hear from today's witnesses is when will the Department finish the National Infrastructure Protection Plan? Our Chairman alluded to this plan. The levee systems are not included in that plan. We had some, as you know, miniature golf courses that were on the plan, and I can't see how we can put a miniature golf course on this infrastructure protection plan but we can't put a levee system on the plan. Andy Purdy from the Department testified 2 days ago that he couldn't tell us definitively when it was going to be completed. I hope you can do better than that.

GAO and IG both have looked at the National Infrastructure Plan, and they said it is inadequate. It is back in the Department for further review. We were told initially we might get it by November; now we hear February, but I would like to know for sure when that time is.

I yield back.

Mr. LUNGREN. Thank you, Mr. Thompson.

Mr. LUNGREN. We are pleased to have two members for a distinguished panel of witnesses before us today on this important topic, and the Chair recognizes Mr. Robert Stephan, the Acting Under Secretary for Information Analysis and Infrastructure Protection of the U.S. Department of Homeland Security to testify.

STATEMENT OF ROBERT STEPHAN

Mr. STEPHAN. Thank you, Mr. Chairman. Good afternoon. And good afternoon to you, Representative Thompson. I appreciate the opportunity to speak with you and your distinguished committee today.

The Department of Homeland Security, I assure you, is committed to working with our partners in State and local and tribal governments, as well as across broad elements of the private sector to reduce the overall level of risk of terrorist attacks against our national critical infrastructure and key resource base.

In analyzing terrorist risk, it becomes clear that certain means of attack against certain types of targets are easier for terrorists to accomplish and execute, and more difficult for us to protect against. The July 7th and 21st horrific attacks on the London mass transit system in 2005, as well as the March 2004 attacks in Madrid, underscore the inherent vulnerability of so-called open-access systems.

Recognizing that despite our best efforts we cannot always protect everyone and everything against all dangers, Secretary Chertoff's risk-based approach allows us to make better judgments about where we target resources, and prioritize our protection ef-

forts to reduce this overall risk, and protect our critical infrastructures and key resources from terrorist attacks.

In doing so, DHS has several principle objectives in mind: providing resources and training to State and local governments and law enforcement for security enhancements across the board; providing information to both public and private sectors on the threat environment, the tactics, techniques and procedures of terrorist organizations and terrorist individuals, our common vulnerability and risks, suggested protective measures; as well as creating information-sharing networks and mechanisms that efficiently and effectively enable DHS to share best practices, as well as our Federal Government partners in the unique aspects of their assets, to improve situational awareness during a crisis or when faced with a general or a specific threat situation.

These objectives are being realized through the implementation of a Unified National Plan—and I will answer Representative Thompson's concerns regarding the National Infrastructure Protection Plan in follow-along questions, sir—for the consolidation of critical infrastructure protection activities into your basket that we are responsible for. The cornerstone of this National Infrastructure Protection Plan is a risk management framework that combines threat, vulnerability and consequence information and approaches to produce a comprehensive, systematic and informed assessment of national and sector-specific risks that drive our risk reduction efforts in the critical infrastructure and key resource sectors.

The principal steps in this risk management framework are to set sector security goals, identify assets, assess risks, and prioritize our efforts and resources accordingly based on the severity and mass effect of potential consequences principally, although, importantly, also taking into account vulnerabilities and specific threat information.

DHS has developed two important tools to assist in this process. The first of these is the National Asset Database, the central Federal repository for national infrastructure-related information that we get from a host of stakeholders across State, local and private sector arenas, and serves also as an inventory of the Nation's assets and infrastructures.

Secondly, we have a risk management tool called RAMCAP, which is an acronym for risk assessment and management for critical asset protection, which is collaboratively being developed across sectors that will guide and provide a spearhead for this national risk assessment, Mr. Chairman, that you are looking so desperately for, to enable an assessment and comparison of risk of critical infrastructure assets both across and within our most important sectors of responsibility, thereby enabling the prioritization of protective efforts and resources, and a more efficient conduct of our responsibility.

DHS leads the Federal Government's critical infrastructure protection efforts and works in collaboration with State and local governments, the private sector, and, of course, numerous other Federal departments and agencies. We are not lone wolves in this mission.

Examples of protected programs DHS has implemented successfully and will continue to execute upon include the DHS Vulner-

ability Identification Self-Assessment Tool, which has a very broad application across these open-access targets that you are very concerned about with this hearing. The goal of this program is to raise the level of security awareness in public assembly facilities across the Nation, as well as establish a common baseline of security from which these facilities can build their protection plans and their appropriate response mechanisms with Federal, State and local partners.

We also have a Target Awareness Training Program that provides baseline prevention and awareness training to first-level supervisors and security personnel across these so-called soft target categories in order to increase their ability to deter and detect potential attacks, as well as increase the reporting of suspicious activity and suspect items.

One of the principal goals of our Federal, State, local and private sector partnership is providing the necessary framework and support to really enable coordination and information sharing within critical infrastructure sectors across these sectors, and between all levels of government and the private sector in order to achieve and execute our responsibilities.

Examples of various information-sharing mechanisms. Later on in the question-and-answer session, I would love to get in more deeply with you some of the more specific incidents surrounding the London bombings, the recent terrorist threat information relative to New York and Baltimore, if you would like.

Examples of things that we use as information-sharing mechanisms includes sector coordinating councils, government coordinating councils, our Homeland Security Information Network—which our director Matt Broderick will be briefing you on tomorrow—the National Infrastructure Coordinating Center, and various private sector information-sharing and analysis centers.

DHS also has and will continue to work closely with allied nations and international partners with respect to garnering information relative to open-access target sets as well as tactics, techniques and procedures that are employed by terrorist adversaries that more routinely perhaps than in the United States perpetrate devastating attacks abroad against their facilities, assets and open-access systems.

We also are members of the Department of Defense's effort in the Joint Improvised Explosive Device-Defeat Task Force, which is an important interagency, international effort with Israeli, Australian, Canadian and British participation to get at very significant problems.

In terms of reacting to crisis situations in the immediate aftermath of the London attacks on July 7th, DHS activated our Interagency Incident Management Group to serve as the national headquarters-level multiagency coordination hub for incident management and response. Upon the decision to elevate the Homeland Security advisory system from yellow to orange for the mass transit sectors specifically targeted, the Office of Infrastructure Protection, in partnership with the Transportation Security Administration, coordinated outreach with the private sector and public sector partners broadly in the mass transit sector to provide them with an overview of the latest threat intelligence, to explain the implica-

tions nationwide of the move to orange, and to provide them an opportunity to discuss those implications.

We have worked with our Federal partners to enhance security in our Nation's largest mass transit system and transit systems across the board, and have made Urban Area Security Initiative funding available for overtime to State and local law enforcement for activities related to increased mass transit security.

Throughout this process DHS effectively executed a mission during the July 7th and 20th attacks as coordinator of National Critical Infrastructure Protection efforts as well as the national—level focal point for information sharing both within the Federal Government and between the public and private sectors.

In conclusion, I would like to reinforce—and I want to answer many of the important questions you raised in your introductions, gentlemen—that we are dedicated to working with infrastructure stakeholders across the country to increase the security of our Nation's critical infrastructure sectors using Secretary Chertoff's risk-based approach. The places and events where our fellow citizens are most vulnerable are a key priority. With your continued support, spirit of cooperation, as well as that of the American people, we will succeed in this very important issue, and these people are not going to beat us. Thank you.

Mr. LUNGREN. Thank you very much, Mr. Stephan.

[The statement of Mr. Stephan follows:]

PREPARED STATEMENT OF ROBERT B. STEPHAN

OCTOBER 20, 2005

Introduction

Good morning, Mr. Chairman, Ranking Member Sanchez and distinguished Members of this Subcommittee. I appreciate the opportunity to speak with you.

The Department of Homeland Security is committed to working with our partners in State, local and tribal governments and the private sector in reducing the overall level of risk of terrorist attacks against our national critical infrastructure. By reducing risk, we mean examining the consequences of a potential attack; examining the vulnerability of critical sites and facilities to various modes of attack; and examining the potential threat—that is, the intent of terrorists to attack in a given place and their likelihood of success.

In analyzing risk, it becomes clear that certain means of attack against certain types of targets are easier for terrorists to accomplish and difficult for us to protect against. The July 7 and 21 attacks on the London mass transit system in 2005, as well as the March 2004 attack in Madrid, underscore the inherent vulnerability of open-access systems.

Recognizing that despite our best efforts, we cannot always protect everyone against all dangers, this risk-based approach allows us to make better judgments about where we target resources and prioritize our protection efforts.

In working to reduce risk and protect critical infrastructure, DHS has three principal objectives:

- Provide resources and training to State and local governments and law enforcement for security enhancements;
- Provide information to both public and private sectors on the threat environment, tactics and techniques of terrorists, common vulnerabilities and suggested protective measures; and
- Create information-sharing mechanisms that enable DHS stakeholders to share best practices and the unique aspects of their assets to improve situational awareness during a crisis or when faced with a specific threat.

The National Infrastructure Protection Plan

These objectives are being realized through the implementation of the National Infrastructure Protection Plan (NIPP). Directed by Homeland Security Presidential Directive 7 (HSPD–7), the NIPP is a unified national plan for the consolidation of critical infrastructure protection (CIP) activities. The NIPP is a collaborative effort

between the private sector, State, local, territorial and tribal entities and all relevant departments and agencies of the Federal government.

The cornerstone of the NIPP is a risk management framework that combines threat, vulnerability, and consequence information to produce a comprehensive, systematic, and informed assessment of national or sector risk that drives our risk reduction efforts in the critical infrastructure/key resources (CI/KR) sectors. This framework applies to the general threat environment as well as specific threats or incident situations.

NIPP Risk Management Framework

Set Security Goals. Achieving a secure, protected, and resilient infrastructure requires a common set of national and sector-specific security goals that address those aspects of risk that can be affected and collectively represent an acceptable security posture. Therefore, sector security goals will be determined through a collaborative effort of government agencies and the private sector. Establishing sector security goals is the nexus of the NIPP planning process that will drive the public/private partnership. Nationally, the overarching security goal of reducing risk begins with an enhanced state of CI/KR security, a state which is best achieved through the implementation of focused risk reduction and protective strategies across the critical sectors.

Identify Assets. Once security goals are set, the next step in the framework is to develop and maintain an inventory of the Nation's assets. First, asset information is collected and catalogued in the National Asset Database (NADB), which is the central Federal repository for national infrastructure-related information. Second, after an asset is identified and basic information on it is collected, DHS employs an initial screening methodology to determine whether or not it is of national consequence. Finally, priority is given to applying federal resources to those assets that, if attacked, could have a nationally significant effect.

Assess Risk. If an asset is determined to be of national consequence, it is then subjected to a risk analysis. As mentioned before, risk is determined through a combined assessment of:

- Consequence—estimates of the damage a successful attack would cause;
- Threat—estimates of the likelihood that a particular target or type of target will be selected for attack; and
- Vulnerability—assess which elements of infrastructure are most susceptible to attack and how attacks against these elements would be most likely carried out.

One of the Department's principal risk-assessment tools is RAMCAP (Risk Assessment Methodology for Critical Asset Protection). RAMCAP is being developed by DHS in collaboration with other federal agencies and the private sector as a sector-specific consequence, vulnerability, and risk methodology. RAMCAP enables an assessment and comparison of risk of critical infrastructure assets both across and within CI/KR sectors, thereby enabling the prioritization of protective efforts and effective use of available resources.

Prioritize. It is impossible, nor do we attempt, to protect all CI/KR equally across the entire United States. We assess the potential consequences of an attack, threats, and vulnerabilities for CI/KR sectors, as well as individual assets within those sectors and prioritize our efforts based upon the severity and mass effect of potential consequence. Conducting risk analysis provides us with the information needed to make such determinations, as well as provides the department a basis upon which to make longer-term resource decisions including strategic protective programs and planning for response and other contingency situations.

Implement Protective Programs. The widely dispersed nature of critical infrastructure demands equally dispersed ownership and execution of protection programs. It requires centralized leadership which in turn drives consistent implementation and ensures the greatest cost-benefit through addressing the greatest risks. DHS leads the Federal government's critical infrastructure protection effort, and works in collaboration with State and local governments, the private sector, and our international partners to protect against potential terrorist attacks through reducing our vulnerabilities and enhancing our response capabilities to potential terrorist attacks. Some of the key DHS programs include:

- **Vulnerability Identification Self-Assessment Tool**—An important initiative designed to increase the capabilities of private sector owners and operators to enhance their own security is the DHS Vulnerability Identification Self-Assessment Tool (DHS–VISAT). This is a voluntary, on-line assessment tool that was originally developed to help transportation asset owner/operators enhance security. The goal of this program is to raise the level of security awareness in public assembly facilities across the nation and establish a common "baseline"

of security awareness from which these facilities can build their protection plans. To date, it has been adapted for use by stadium and arena managers and access has been provided to over 300 stadiums and 400 arenas. Currently this tool is being modified for use by other commercial venues including convention and performing arts centers. In addition, we have engaged in piloting efforts with the States of Texas, Virginia, and California to adapt the tool to support security awareness in K–12 schools.

• **Target Awareness Training**—The Target Awareness Training (TAT) program provides baseline prevention and awareness training to first level supervisors and security personnel and is supported by VISAT. The primary objectives of TAT are to increase the ability to deter and detect potential attacks and to increase the reporting of suspicious activity and suspect items. The courses focus on law enforcement and security staff working in shopping malls and centers, places of worship, educational institutions, hotels, and sports complexes. Over 2,500 law enforcement and private sector personnel have participated in 128 TAT Courses since September 2003. We also provide a Surveillance Detection Course, Surface Transportation Antiterrorism Program, and an Improvised Explosive Devices/Weapons of Mass Destruction (IED/WMD) Electronics course.

• **Bomb Prevention**—Bombing is a preferred tactic for terrorists seeking relatively uncomplicated, inexpensive means for harming large numbers of people and inflicting maximum damage on critical infrastructure. The threat that IEDs and other types of explosive weapons pose are of great concern given the relative technological ease with which such an attack could be planned and executed. Central to preventing bombing attacks are:

• the need for new critical thinking and analysis regarding the nature and scope of preventing an attack;

• innovation in detection, deterrence, and improving system robustness in the face of an adaptable enemy;

• the importance of increased stakeholder participation and cooperation;

• the need for more robust information sharing and collaboration measures; and

• meaningful dialogue between State and local jurisdictions and the Federal government to identify and fill operational capability gaps related to training, equipment, technology and resources

We will continue to assist state and local entities in identifying gaps in protective capacity and obtaining required resources. Under Homeland Security Presidential Directive-8 and the National Preparedness Goal, the Department is identifying bomb prevention capabilities at every level of the government and identifying gaps in this capability. We are taking steps to address any gaps that exist by developing a focused and unified national bombing prevention effort through such groups as the Interagency Governance Board and the IED Task Force. DHS is also developing enhanced knowledge management systems that foster information sharing and collaboration between Federal, State, and local entities involved in bombing prevention, and among various and disparate law enforcement jurisdictions.

Information Sharing

One of the principal goals of the Federal-State-local-private sector partnership is to provide the necessary framework and support to enable coordination and information sharing within each CI sector, across all CI sectors, and between all levels of the government and private sector in order to achieve the execution of a full spectrum of prudent and responsible protective actions.

• **Sector Partnership Model**—Under the NIPP framework, DHS is helping to create private sector-led Sector Coordinating Councils (SCCs) for each of the 17 critical infrastructure sectors. These councils will serve as a mechanism for identifying risk and protection issues within their specific sector and addressing the range of infrastructure protection activities. For example, the "Commercial Facilities" sector coordinating council encompasses open-access facilities that, if attacked, could cause significant casualties and economic damage. Accordingly, membership in the Commercial Facilities SCC includes all major sports leagues, International Council of Shopping Centers, Marriott, Warner Brothers, Disney, the Real Estate Roundtable, the Self Storage Association, the International Association of Assembly Managers, and others.

Both the SCCs, and their government counterparts, Government Coordinating Councils (GCCs) will increase inter-agency coordination and information sharing on critical infrastructure protection activities. The GCC coordinates strategies, activities, policy, and communication across organizations within each sector. Unlike the SCC, it does so through the Federal government. The SCC and GCC work together to create a coordinated national mechanism for infrastructure protection in their sector. Members of the Commercial Facilities GCC include the US Secret Service,

the Federal Protective Service, the Environmental Protection Agency, the General Services Administration, and the Departments of Commerce, Justice, Interior, and Education.

• **Homeland Security Information Network**—DHS is developing a networked approach to information-sharing that enables rapid information dissemination to decentralized decision makers across the nation. The key objectives of this approach are to enable multi-directional information sharing between and across government and industry; provide all CI/KR sector owners and operators with a robust communications framework, tailored to the specific information sharing requirements of each sector; and provide a comprehensive threat landscape to all security partners, including general and specific threats, incidents and events, impact assessments, and best practices.

At the core of this networked approach is a series of sophisticated, secure tools and support mechanisms, collectively referred to as the Homeland Security Information Network (HSIN), which provides a national communications platform that enables the flow of near real-time information among governmental entities at all levels (i.e., Federal, state, territorial, local, and tribal), private sector organizations, and international security partners.

• **National Infrastructure Coordinating Center**—The National Infrastructure Coordinating Center (NICC) is a 24x7 watch operation center that maintains operational and situational awareness of the Nation's CI/KR sectors. The fully operational NICC provides a centralized mechanism for gathering information and a process for sharing and coordinating information between and among government, SCCs, GCCs, and other industry partners. The NICC receives incident reports from specific sectors in accordance with pre-established information-sharing standard operating procedures. When required, the NICC also disseminates a wide range of products containing warning, threat, and critical infrastructure protection (CIP) information to the private sector and government entities. The NICC is also responsible for receiving situational and operational information from the private sector and disseminating that information throughout the Homeland Security Operations Center (HSOC), other government operation centers, and industry partners as applicable.

• **Information Sharing and Analysis Center**—The private sector has established a number of information-sharing mechanisms that contribute to the protection of their assets. One such mechanism is the Information Sharing and Analysis Center (ISAC). While the SCCs ultimately define the unique information-sharing requirements for each sector, ISACs and other existing mechanisms provide an array of options and capabilities for some infrastructure owners and operators.

ISACs, while varying greatly in composition, scope, and capabilities, offer a viable information-sharing mechanism. Some ISACs, for example, maintain 24x7 watch centers and provide various levels of sector-specific alerting and analysis. In this regard, the Surface Transportation and Public Transportation ISAC collects, analyzes, and distributes critical cyber and physical security and threat information from government and numerous other sources on a 24/7 basis. Other ISACs maintain a watch center that is staffed during traditional business hours, with the ability to contact analysts via telephone or pager during periods of increased activity. Still others operate primarily through Websites, allowing members to access sector-related alerts, warnings, and incident information. Regardless of the variance in breadth and depth, however, ISACs are capable of disseminating DHS-issued threat information.

• **International Information Sharing**—We have made significant progress in cooperation with our international partners in the war on terror to share best practices and intelligence. This is especially true in the area of bombing prevention. The United Kingdom and Israel have years of experience in bombing prevention. DHS has and will continue to work closely with Scotland Yard and the Israeli Defense Force and police in order to learn better methods of bombing detection and prevention.

Additionally, we are part of the Department of Defense's effort in the Joint Improvised Explosive Device-Defeat Task Force, an interagency, international effort with Israeli, Australian, Canadian, and British participation. The task force will establish an open-door program of international partners who will work to develop and exchange detection and prevention technologies.

Reacting to Crisis

In the immediate aftermath of the July 7, 2005, attacks in London, DHS stood up the Interagency Incident Management Group (IIMG) to serve as the national headquarters-level multi-agency coordination entity for incident management. Secretary Chertoff then recommended to the President that the Homeland Security Ad-

visory System (HSAS) move from YELLOW to ORANGE for the Mass Transit Sector. In response, the Office of Infrastructure Protection, in partnership with TSA, coordinated outreach with public and private sector owners and operators in the Mass Transit Sector to provide them with an overview of the latest threat intelligence, to explain the implications of a move to ORANGE, and to provide them an opportunity discuss those implications.

We worked with our Federal partners to enhance security at our Nation's largest mass transit systems and made Urban Area Security Initiative (UASI) funding available for overtime to State and local law enforcement for activities related to increased mass transit security. Our intelligence and analytical units produced Joint Advisories and Information Bulletins with the FBI that detailed what we knew about the terrorists target selection, attack methodology, implications, and suggested protective measures that mass transit operators could implement. Following the attacks, personnel from the Office of Infrastructure Protection and TSA conducted analysis of mass transit systems, starting in large cities such as the New York and New Jersey systems. Inspectors from the Federal Railroad Administration conducted inspections of passenger rail operations in the days immediately following the July 7 attacks. Throughout this process, DHS effectively executed its mission as a coordinator of national critical infrastructure protection efforts, and served as the focal point for information sharing both within the Federal government and between the public and private sectors.

Conclusion

DHS is dedicated to working with infrastructure stakeholders across the country to increase the security of our Nation's critical infrastructure sectors using a risk-based approach. The places and events where our fellow citizens are most vulnerable are a key priority. With your support and that of the American people, we will succeed. Thank you.

Mr. LUNGREN. The Chair would now recognize Mr. Robert Jamison, the Deputy Administrator, Transportation Security Administration of the U.S. Department of Homeland Security, to testify.

STATEMENT OF ROBERT JAMISON

Mr. JAMISON. Good afternoon, Mr. Chairman and Mr. Thompson. I am pleased to appear before you in my new capacity as the Deputy Administrator for TSA to testify on the critical subject of protecting civilian targets from terrorist attack. My testimony this morning will focus on our approach to accomplishing this mission, focusing particularly on public transportation.

At the outset, I want to acknowledge the team nature of security in today's world and express appreciation for the work of the Department of Transportation and our partners in State and local government and throughout the transportation industry.

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

Despite the good work that has already been done in improving security in transit, the London bombings and other events throughout the world have demonstrated the need for a new strategic approach to transportation security. Fundamentally our challenge is to protect our transportation network in a constantly changing threat environment. We understand better that terrorists will not only look for weaknesses in our transportation system and in security measures, but they will also adapt to perceived security meas-

ures. As a result, it is not possible to precisely predict with any degree of certainty the next attack based on previous terrorist activity.

In the face of this unpredictability and rapid change with respect to threats, our approach to security in every transportation sector must be based on flexibility and adaptability. While it is necessary, it is no longer sufficient to protect ourselves against known or suspected terrorists; we must protect ourselves against people with no known affiliation to terrorism. While it is necessary to, it is no longer sufficient to focus on finding threat devices like guns and explosives; we must enhance our ability to find terrorists before an attack is underway. And while it is necessary, it is no longer sufficient to subject every passenger to basic security procedures; we must create uncertainty, an element of unpredictabilty in our security operations, in order to disrupt terrorist planning and attempts.

To accomplish these objectives, TSA is pursuing a security strategy based on Secretary Chertoff's Second Stage Review. There are four cooperating principles applicable to TSA. First, we will use analysis based on risk vulnerability and consequence to make investment and operational decisions. Second, we will avoid giving terrorists an advantage based on our predictability. TSA will deploy resources, such as K–9s and air marshals and inspectors, for example, and establish protocols, standards and best practices flexibly based on risk. Terrorists will not be able to use the predictability of our security measures to their advantage in carrying out an attack.

Third, we will continue to intervene early based on intelligence, law enforcement information and suspicious incident reporting that focus our security measures on the terrorist as well as the means for carrying out the threat. Effective analysis and dissemination of timely information to those in need is a vital component of this effort.

Finally, we will build and take advantage of security networks. We are pursuing a restructuring of TSA that will put renewed emphasis on building on information-sharing networks in every transportation sector. Through these efforts, we will work more closely with stakeholders and put a renewed emphasis on sharing intelligence, capacity and technology with other law enforcement, intelligence-gathering and security agencies at every level of government. We will build a more robust, distributed network of security systems to protect America.

As we move forward, we are fortunate to be able to build on solid foundation not only at the local level, but nationally as well. This foundation includes products and resources developed by our Federal partners, especially at the Department of Transportation, with the Federal Transit Administration and the Federal Railroad Administration, and partners in the industry at the American Public Transportation Association, the Association of American Railroads and its members, labor unions, and individual public transportation systems. This collective expertise fortifies their knowledge, expertise and overall strategic approach. We value the critical role of Congress and especially this subcommittee, that this subcommittee plays in this effort, and we look forward to working with you on a full range of these issues.

I am happy to appear, and I would be pleased to answer any questions you might have.

Mr. LUNGREN. Thank you very much.

[The statement of Mr. Jamison follows:]

PREPARED STATEMENT OF ROBERT JAMISON

OCTOBER 20, 2005

Good afternoon, Mr. Chairman, Congresswoman Sanchez, and Members of the Subcommittee. I am pleased to have this opportunity to testify on the subject of "The London Bombings: Protecting Civilian Targets from Terrorist Attack." As requested, my testimony today will focus largely on public transit and intercity freight and passenger rail transportation.

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

Overview of Surface Transportation

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

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

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

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

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

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

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

with stations serving rail transit, intercity bus, and other modes of transportation. Amtrak operates over more than 22,000 route miles. It owns 650 route miles, primarily between Boston and Washington, DC, and in Michigan. In other parts of the country, Amtrak trains use tracks owned by freight railroads.

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

London Lessons Learned

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

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

The London attacks were particularly noteworthy from a security perspective.

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

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

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

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

Adapting to a Changing Threat Environment

Despite the work that has already been done, Mr. Chairman, the London bombings and other events throughout the world have demonstrated the need for a new strategic approach to transportation security. Fundamentally, our challenge is to protect passengers, freight, and our transportation network in a constantly changing threat environment. We understand better that terrorists will not only look for weaknesses in our transportation system and its security measures, but they will

also adapt to perceived security measures. As a result, it is not possible to "predict" the next attack based on previous terrorist activity or put into place specific security measures to protect against it. In this dynamic environment, history is an unreliable guide.

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

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

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

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

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

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

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

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

- TSA will identify opportunities and engage the private sector in its work to develop and implement security systems and products.
- We will protect the privacy of Americans by minimizing the amount of personal data we acquire, store and share, and we will vigorously protect any data that is collected, stored or transmitted.
- And TSA will remember, in all that we do, our goal in stopping terrorism is to protect the freedoms of the American people. Therefore, we will work to make

travel easier for the law-abiding public, while protecting the security of the transportation network and the people who depend upon it.

A Solid Foundation

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

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

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

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

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

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

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

tasks, the security compliance inspectors will identify gaps in security and validate compliance with TSA's security directives.

Conclusion

Mr. Chairman and Members of the Subcommittee, I want to assure you that TSA is pursuing a robust strategy to support rail and transit security that builds upon the work of other Department of Homeland Security agencies, the Department of Transportation, and our public and private sector partners at the State and local level. We look forward to working with Congress and this Committee as we continue to protect America's transportation infrastructure, its passengers, and the commerce that depends upon it.

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

Mr. LUNGREN. We only have the two of us here, but I will sort of go by my 5-minute rule so we can go back and forth on this and spend as much time as we need.

Mr. Stephan, do you prefer being referred to as Colonel Stephan?

Mr. STEPHAN. Either one.

Mr. LUNGREN. Well, I think someone who has earned that title ought to be able to keep it; so if you don't mind, I will call you Colonel.

Mr. STEPHAN. All right, sir.

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

We have had this question about the National Infrastructure Protection Plan and sector-specific plans due by the end of the year. When are we actually going to see them? And plans are all well and good, but what do you do with them? I mean, what is the added value to those plans over and above what your Department is doing or what sectors are doing themselves individually?

Mr. STEPHAN. Yes, sir. This subject is very near and dear to me, and I want to be very up front and candid with both of you gentlemen.

I took this job—the most significant responsibility I think I have had in my life—the end of April of this year. The strategic backbone document for everything I am supposed to be doing is something called the National Infrastructure Protection Plan. I grabbed ahold of that document in the early May time frame in its interim form that the Department issued in February, and as I read the document, a sinking feeling rapidly came over me. I took the document and I compared it to what the requirements that President Bush set forth clearly, very clearly articulated in HSPD–7, and the document was simply missing in action 50 percent of what I believe the President clearly articulated needed to be in that document, in HSPD–7. And the document appeared to me to be yet another one of these never-ending series of documents that tell us what has to be done. After multiple years have passed since September 11th attacks, everyone in this room knows what has to be done. The question that document has to get to is: How are we going to do the whats that are listed in the document?

So doing this the only way I know how to do it—and I have developed or led the development of three other national plans or strategies at this level—I took the document, I got a new team. It is not a team of contractors, it is a team of government employees that have helped me with previous plans. I have got them firmly under my direction, and we have worked that document over the last several months to include some very important missing-in-action items.

We very clearly articulate now in this document what the roles and responsibilities of various State and local players in all of this and private sector players are; the international dimension; the cyber dimension; how the Federal budget infrastructure protection should come together in some kind of logical, meaningful way, a series of metrics, a series of things that will hold people accountable, deliverables, timelines. All of this, I am happy to report, I completed with my team last week, and I have turned it in to Department Secretary Jackson and Deputy Secretary Chertoff for their review.

Prior to this, I conducted a broad review across our Federal Interagency Senior Leadership Council and have gotten back from them on a one-for-one Q&A session with no significant pushback on anything in the plan.

What I need to do now is, upon release authority from the Secretary and the Deputy Secretary, is allow this plan in final draft form to go out for about a 30-day comment period to a broad gathering of State, local, tribal government partners and the private sector folks so I get their opinions, because the previous version of this document was not very broadly coordinated as it should have been across the very wide stakeholder community. I owe that to those people, so I am going to do that when I get the send button pushed from the Secretary. I hope to get that very, very soon.

I will take the comments that come back from that process, and if there are significant comments, I will propose a second round of coordination across that stakeholder community. And I want to put the final pieces of this together as quickly as I can towards the end of the year or the first of the year, to be as frank and honest as I can with you. That will be depend on the level of comment that I get across the private sector and across our State and local government partners.

I firmly believe in this document. If we don't have this document, we have no strategic backbone. We don't have the "hows" answered. We need to figure out how we are going to operationalize this risk assessment piece that is now in this plan. We have to figure clearly and clearly state who is responsible for what, that is in this plan; how our resources come together; and how they are wisely targeted against the broad array of critical infrastructure and key resources.

Mr. LUNGREN. You appreciate the frustration of Members of the Committee when they hear that this is the strategic backbone, and here we are 4 years after 9/11 and we don't have it yet?

Mr. STEPHAN. Yes, sir. And I can say to you personally that no one in this room is more frustrated than I am personally by this, sir. And it is my job to fix it. I own this operation now, and it is going to be fixed. And it is on my boss's desk.

Mr. LUNGREN. I looked at your bio, and I noticed that you had been involved with contingency operation planning in Somalia, Haiti, Bosnia, Croatia, Liberia, Colombia, Kosovo. You have been the one that has been involved in that kind of planning in the past as part of your military experience.

Mr. STEPHAN. Yes, sir.

Mr. LUNGREN. And I take it from what you are saying you have tried to apply that same sort of military rigor to this planning even though you arrived late at the process?

Mr. STEPHAN. Sir, it has to be a very rigorous process. And I led the development of the President's Strategy for Critical Infrastructure Protection in the year 2001 and 2002. I know how to do this. I spent a lifetime trying to attack other people's target sets. I have to reverse-engineer that across the United States. And the defensive team is challenging, a lot more challenging than the offensive has it.

Mr. LUNGREN. You see what happens here in the Committee, we look at DHS as sort of an amorphous operation, and when we have heard this plan is going to be coming out, it is going to be coming out, it is going to be coming out, we tend to look with a little skepticism about another repeat that "it is going to come out". But what I am taking from what you are saying is you arrived late to the game, you found somethi ng that looked like a fumbled football, and you picked it up, and you are trying to bring it forward; would that be correct?

Mr. STEPHAN. Sir, I realize the importance of this document and how important it is to the country, and I realize I am not going to get another chance to get it right. And I am going to get it right with my team.

Mr. LUNGREN. It was not right when you picked it up.

Mr. STEPHAN. I don't believe it was accurate; it did not meet President Bush's thoroughly articulated criteria that appeared in HSPD–7.

Mr. LUNGREN. Well, this is the President's clearly articulated criteria. What about your sense of what you needed to do to have a mission understood and carried out?

Mr. STEPHAN. No, sir, it was not an operational document. This document was more akin to a strategy, broad-level strategy document that we have multiple copies of those kinds of things floating around the Federal Government. This needs to be an operational plan that everybody understands, knows what their part is, knows how resources come together, how they are applied, how we are going to focus, what risk assessment criteria we are going to use as a standard across the Nation. That is what this has to be. And I believe Bob Stephan has produced what it needs to be, and it is sitting on my boss's desk right now.

Mr. LUNGREN. The Ranking Member is recognized for 5-plus minutes.

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

Colonel, I appreciate your truthfulness. And I think this committee supports the effort to come up with a document that we all can feel proud of. Anything less is not acceptable. I don't think you will have any problem from this committee pursuing exactly what you see as that mission and the production of the plan.

I had a couple of questions I wanted to ask. Mr. Jamison, I actually had a hazmat question to ask you, and I was told I can't ask you this question as you have a conflict. Any idea on when you are going to get the conflict resolved so I can get my question answered?

Mr. JAMISON. I would be happy to provide an answer to you for the record. Unfortunately, this is my first day on the job at the Transportation Security Administration, so I am still going through the ethics process, and as soon as I am through with that process, I will be able to answer your question. But I will be happy to provide an answer to you for the record.

Mr. THOMPSON. Can you give me some kind of time frame on when you will have it resolved?

Mr. JAMISON. I am hoping to have it resolved in the next several weeks.

Mr. THOMPSON. And that conflict doesn't prevent you from doing your job?

Mr. JAMISON. It does not prevent me from doing my job. I am recused from certain matters until that conflict is resolved, but I am able to execute the duties of the job.

Mr. THOMPSON. All right. Thank you very much.

In the 9/11 Commission report and the legislation that came from that, we require a plan to be developed for transportation security, a strategy. When will Congress see that strategy?

Mr. JAMISON. They received the strategy in September, which is the National Strategy for Transportation Security, which was submitted. After Mr. Stephan submits his National Infrastructure Protection Plan, I believe it is 180 days after that it will be updated, but the strategy was received.

Mr. THOMPSON. So it is your testimony that we now have that strategy?

Mr. JAMISON. You have the National Transportation Security Strategy.

Mr. THOMPSON. Well, Mr. Chairman, I have a list of questions I would like to submit for Mr. Jamison to answer because what we have is not a strategy. We have some elements, but we don't have a strategy. But I will accept your word on it and just pursue it at a later date.

Mr. THOMPSON. In addition to that, this committee heard testimony earlier in the week relating to some intelligence questions around collection and analysis as it relates to transit security with both New York City and Baltimore. We were a little troubled that there appeared to be a disconnect between the transit security system and the Department of Homeland Security intelligence-gathering system and the city of New York. Have you had—and I know this is your first day on the job, but have you had an opportunity to look at that disconnect? If so, can you tell us how we can fix it?

Mr. JAMISON. Well, while I was involved in my role in DOT in that event—and I think the lesson learned from London is even one of the most prepared systems in the world at a heightened state of alert, it is very difficult to prevent attacks on mass transit. So it is very important that the shared responsibility of security between Federal, State and local, that we share information as quickly as we can and get as much information to the State and locals and have them make a decision they need to make.

In this instance that was done quickly, the information was shared. In addition to the information, an analysis portion, which the Federal Government plays a key role in, was shared with the New York officials. And it is their role—and I respect that role—

to take that information and weigh the risk in their local areas versus the information and make decisions to take action.

Mr. THOMPSON. So do you agree with what they did?

Mr. JAMISON. I respect the decision. I mean, the analysis that we gave them was given in an effort to enable them to make decisions.

Mr. THOMPSON. I will ask you one more time, did you agree with the decision they reached, yes or no?

Mr. JAMISON. I agree that they have the right to make that decision. The issue on whether or not they have the right to deploy the resources, absolutely, I agree that they should have deployed resources if they felt like that was their responsibility.

Mr. THOMPSON. Well, one of the things we keep hearing is we don't have enough connectivity between all these agencies; even though we passed legislation that mandated it, we still don't see it. At their press conference that Mayor Bloomberg had, the FBI was standing next to him, but not DHS. I am trying to figure out whether you agreed with it or you didn't. Does your absence at this press conference signify that you didn't agree with it?

Mr. JAMISON. Well, again, Congressman, I think this is a positive story that the system worked, that the information got down to the local levels, it got to the local levels quickly, they were able to assess it and make decisions. You know, I was not in Mayor Bloomberg's shoes—

Mr. THOMPSON. Were you invited to the press conference?

Mr. JAMISON. Was DHS invited to the press conference? I don't know that. I don't know the answer to that.

Mr. THOMPSON. Mr. Chairman, can we, for the record, find out from DHS if they were invited to this process conference that Mayor Bloomberg had? I think it would be important.

Mr. LUNGREN. I am sure you can let us know whether you were invited or not.

Mr. JAMISON. Absolutely.

Mr. THOMPSON. Your absence at the press conference would indicate a lot, given the information you provided New York City.

Thank you, Mr. Chairman.

Mr. LUNGREN. Mr. Pearce, are you ready to inquire?

Mr. PEARCE. Thank you, Mr. Chairman—

Mr. LUNGREN. We have a loose 5-minute rule, more than 5.

Mr. PEARCE. Thank you very much. That differs from some committees, and I appreciate the Chairman's—

Mr. Harley, the Transportation Security Administration just recently did a field test of the—we don't have Mr. Harley. Mr. Jamison. The TSA ran the puffer machines. I have seen one of those. They had, I think, one at Mount Vernon—not Mount Vernon, the Statute of Liberty—and I wonder how those machines are working and the effectiveness and what the cost on those is.

Mr. JAMISON. We did run what we deem as a successful test called Trip on the puffer machines, and actually a three-phase test. The first part was in New Carrollton, Maryland. And the major success part of the test is that we were able to take that technology, the puffer machine that is usually used in aviation, and adapt it to the transportation environment. It did work in that arena; however, there still remain a lot of problems with deploying that technology in the security or in the transit environment.

One, the throughput, it takes 15 seconds or more for each passenger to go through that system, and it was tested in very low-volume conditions. So in an environment such as New York City, Penn Station, where you have 1,500 people a minute coming into a system through various entrances, it is just not practical to deploy that type of technology.

We are continuing to research the technology, continuing to try to find ways that we get better throughput and develop the alternatives, but at this point there is no current plans to deploy that technology in the transit environment.

Mr. PEARCE. What is the basic cost on those units? And then if we could work out some of the problems, what cost are we looking at broad scale?

Mr. JAMISON. I don't know what the individual cost of the units are. I would be happy to provide that for you for the record. They are expensive.

Mr. PEARCE. Multiples of where we are right now?

Mr. JAMISON. Excuse me. I just got the answer to your earlier question. It is $125,000 per unit.

Mr. PEARCE. And how does that compare to some of the screening mechanisms we are currently using? Is that a multiple of two or three or the same?

Mr. JAMISON. Do you mean in the aviation environment?

Mr. PEARCE. Mm-hmm.

Mr. JAMISON. Actually, it is a multiple of two on some of the technology screening.

Mr. PEARCE. About $65,000 versus $125,000.

If you we look at some of the screening devices that we are using at the airports, we look at the time that it takes there plus the labor intensity, do you see any emerging technologies that can detect the same thing the puffers do, the explosives or weapons? Are we seeing any technologies coming out of that?

Mr. JAMISON. We are carefully evaluating all the technologies that have been used in the aviation arena to see whether or not they are applicable in the transit environment, like backscanner and other types of technologies, to see if we can get high volumes of throughput. But based off of the evaluation currently, we don't see any near-term technology that is going to come up that is going to give us an opportunity to apply it in the transit environment.

Mr. PEARCE. What are the European nations doing with regard to transit safety? Are they doing anything at all?

Mr. JAMISON. There are some contemplating some technology deployments, as pilots only, and we are working closely with them. I was just on a trip overseas to London, and lessons learned, and we were discussing with them what some of the options are, but they currently don't have that technology deployed in London.

Mr. PEARCE. If there is none of the technology deployed, what is the basic philosophical outlook on safety in the mass transit system?

Mr. JAMISON. Well, first of all, I mean, I think the mass transit systems are more secure than they have ever been. What London did was validate that the approach to try to get the terrorists before they get to the system is the most effective strategy, and we need to continue to receive good intelligence and so forth. They also

validated that the focus that we have had on training, awareness training, and making sure that your operators know how to spot suspicious behavior and know how to report it and know how to react, in addition to public awareness campaigns, and in addition to emergency preparedness so that you know how to respond and mitigate the impact of an event are still the most effective strategies.

Mr. PEARCE. And are we prepared in your agency to come to the conclusion that you might not—it might not be able to provide 100 percent fail-safe screening mechanisms; that the cost would be too prohibitive, and there are too many other access points? Are we prepared in this Nation and in your agency to have an open discussion about whether or not we can and should? Because it sounds like that is where Europe already is; that they may employ some things, but they are definitely not sitting here at the cutting edge of technology and approaching it the way we are.

Mr. JAMISON. That is correct. And as I mentioned before, I think we must continue to look—to put research money into technology and to try to determine what the opportunities are to continue to improve the security. But currently more boots on the ground, awareness training, other types of methods are most effective, and screening is not the solution in the near term.

Mr. PEARCE. I see my red light blinking, Mr. Chairman. How loose is your parameter here?

Mr. LUNGREN. I just understand that Mr. Thompson has to leave, so I was going to let him inquire, and then—

Mr. PEARCE. Let me yield, and then if we have a second round, I will take another turn. Thank you, Mr. Chairman.

Mr. LUNGREN. Mr. Thompson.

Mr. THOMPSON. Thank you very much, Mr. Chairman. I appreciate you allowing me to do this.

A couple more questions, Mr. Jamison. Can you tell me if TSA mandates transit systems to provide security training for its employees?

Mr. JAMISON. There is a security directive that instructs transit agencies to provide training to their front-line employees, yes.

Mr. THOMPSON. Do you interpret "instruct" to mean "require"?

Mr. JAMISON. It is a security—it is a legal, binding security directive, yes.

Mr. THOMPSON. Can you provide this committee with that document that requires transit systems to provide training to its employees?

Mr. JAMISON. Sure.

Mr. THOMPSON. Thank you.

Mr. THOMPSON. Another question. Colonel, at a hearing earlier this summer, we talked about chemical plant security, and I think basically you promised, in response to a question from me, that we would have a plan for chemical security within a few weeks. Can you tell me where we are with that now?

Mr. STEPHAN. What I have done at my level in coordination with the Secretary and Deputy Secretary and the Homeland Security counsel, we have worked out, I believe, internal to DHS what we believe the major pillars of a regulatory framework for the chemical industry would look like in terms of a risk-based approach by facil-

ity, by facility category, by facility type, performance measures. I am ready to discuss with Members of Congress the parameters associated with this.

I don't believe we promised a plan, sir; I believe we promised we would be ready to have discussions with our friends on the Hill regarding a framework that would end up in a piece of legislation eventually.

Mr. THOMPSON. Well, given the fact that our chemical plants, as you know, are vulnerable, we do need to come up, I think, in a short period of time with some kind of strategy for the security of those plants, and I look forward to working with you on it.

Mr. STEPHAN. May I add, whether or not we get authority or not, as part of our sector-specific plan for the chemical industry we will have an option A and a B; an option A if we get regulatory authority through legislation, and an option B if we do not have a set authority. We will work through what our other options are and put that as far as the NIPP.

Mr. THOMPSON. Could you, if it is available, provide us with any of that information? Or maybe, Mr. Chairman, we might need to set up a briefing because a number of our Members have concern about chemical plant security.

Mr. STEPHAN. I would like to give you a briefing, if I could do that.

Mr. LUNGREN. We can set that up.

Mr. THOMPSON. Thank you very much.

Mr. Jamison, earlier, in response to a question dealing with the transportation security strategy, I am aware that a plan was sent to us, it was a classified document, and for some reason we are not able to really address it as we should. I understand it is under review to be declassified, but according to Section 4001 of the 9/11 Act, there were some things that that strategy had to include, and I will read them: Set realistic deadlines to address transportation security needs across all modes, establish clear responsibilities between all levels of government and the private sector, delineate roles and responsibility for response and recovery, and prioritize research and development to ensure that effective technologies are deployed as soon as possible.

Now, our reading of the plan indicates that these requirements are not there, so now can you tell me—if my interpretation is wrong. Can you just tell me if those things are there?

Mr. JAMISON. I don't know that the specific plan gets into that much detail. What I can tell you is it is currently security-sensitive information which should give you access to it for one issue. But also the issues that you just laid out there, the majority of those issues have been addressed in a memorandum of understanding between the Department of Transportation and the Department of Homeland Security, such as roles and responsibilities, research, and so forth and so on. Part of that memorandum of understanding requires that DHS and DOT do an annual plan to prioritize research funding, other resources to make sure that they are coordinated, and focused on risk, and prioritized based off of the resources of both agencies.

Mr. THOMPSON. Mr. Chairman, I would basically submit my question to Mr. Jamison in writing so he can give it back to me in writing. Thank you very much.

Mr. LUNGREN. Thank you, Mr. Thompson. And I am sure, Mr. Jamison, you will respond in writing to the question by the Ranking Member.

Mr. LUNGREN. Mr. Jamison, following the Madrid bombing last year, it is my information that TSA issued 20 security directives to public transit agencies to increase transit security. There has been a suggestion by some observers as to whether or not these directives would be effective in preventing a terrorist attack.

Has TSA had a chance to go back and look at those security directives to see if, in fact, they are sufficient for the purpose that they were issued?

Mr. JAMISON. Well, we continue to look at the security directives. And the security directives were meant to establish a baseline of protective measures, and they are also intended to give agencies some flexibility within those baselines so that they could adapt those directives to their individual operating conditions. But the fundamentals of some of the discussion that we were just talking about, about having aware employees, reporting suspicious activity, utilization of K9 teams and other types of measures, is a good indication of the security directives. We need to continue to look at those, continue to work with the industry and continue to determine what are the most effective security measures.

Mr. LUNGREN. So does that mean you are?

Mr. JAMISON. Yes.

Mr. LUNGREN. I mean, you said you should, but I guess that means you are doing that.

Mr. JAMISON. Yes.

Mr. LUNGREN. Congress appropriated millions of dollars to hire 100 rail security inspectors to enforce these security directives. What is the status of that, and how will they be utilized to improve security of mass transit?

Mr. JAMISON. Currently, 99 of the 100 on board are being processed through the HR process. That is an opportunity to look at the security directives and to continue to analyze the gaps in rail transit. It is also a huge opportunity to improve coordination with our stakeholders and make sure we will get real-time, ground-truth information from the field to determine whether or not the appropriate security measures are in place.

Mr. LUNGREN. What kind of feedback are you getting?

Mr. JAMISON. Generally, the majority of the transit agencies—the overwhelming majority of the transit agencies are doing those measures, all of those awareness measures; and as the program ramps up and we get the opportunity to do more security gap analysis, we hope to get more information that helps us develop a more robust strategy.

Mr. LUNGREN. Colonel Stephan, you stated the Department is focused on a risk-based approach to critical infrastructure protection. You heard my comments at the beginning that I was concerned that IP might have developed a risk-based methodology that focuses on each sector from top to bottom and one sector at the ex-

pense of others. What are you doing to make sure we are doing it across the board?

I mean, risk number 10 in one sector may be less severe than risk number 75 in another; and if we are doing sector by sector my concern is, with the limited amount of resources we have, that we might divert them to a less risk-appropriate target scenario than otherwise.

Mr. STEPHAN. We do not intend to methodically go through one sector at a time sequentially and somewhere, years and years and years from now, get to the bottom of this problem. What we are doing is attacking this at cross sectors now in terms of our data calls and data acquisition efforts with State and local governments and the private sector. We are doing this across all 17 critical infrastructure and key resource sectors that are defined in HSPD–7.

The problem that we face, of course, is getting the data. That is one piece. The second piece is doing something meaningful with that data that would then inform a risk-based approach to planning and resource investments.

What we are working on feverishly is making sure that we can compare these apples and oranges within sectors and across sectors. In order to do that, we have worked with the private sector: first with nuclear energy; the chemical industry, next; liquefied or natural gas; the various modes of transportation; the energy sector, to develop this RAMCAP piece.

This is a risk-assessment technology, a technological tool that, when we get this deployed across all the sectors, we will have a standardized criteria by which these data calls will be supported with consequence information, vulnerability information and threat information that is logical across the sectors. That is my big stumbling block now. We are working diligently. We piloted these first two efforts. It took us about a year to get it right with the energy sector and the chemical piece.

The next versions of these are going to go much quicker; and, again, I want to close this whole piece out within the next year or so in terms of having a risk-assessment module, that we have the same thing in each of the sectors in terms of the standardized criteria that allows me to take the data that people are providing me, put it into a computer, and have the apples and oranges all become apples so I can do this cross-sector comparison.

But we are also not waiting for that. We are also taking by whatever criteria I have now and we recently put out about 3 months ago a data call across all the 17 sectors asking us for based-upon criteria that we put out to them. I will be happy to share this document with the committee.

Agriculture and food, banking and finance, chemical, energy, information technology, emergency services, postal and shipping, the list goes on. What are your top assets systems or networks based upon criteria that is specifically defined for each of these sectors? Give us this information so that we can use it to better inform our buffer zone protection plan grant activities, to inform our operational planning, to inform our information-sharing activities.

So that stuff is all under way now.

Mr. LUNGREN. Let me pick up on the buffer zone protection plan grants. It is my information that the way it is to operate is that

every State will be given 70 BZP slots. That is, the State of California will be given 70, the State of Wyoming will be given 70. Then, within that, each State is supposed to make a determination on their own.

My question is: Is that your understanding of the way it is going to be? And, if so, does that make sense that each State gets 70 slots? That is, that you would presume—and I don't want to pick on Wyoming, but in the previous grants program everybody has analyzed it to show that Wyoming has 7 times or 10 times per capita the amount of grants in the previous homeland security grant funding than New York does. So that is why I will pick on Wyoming.

Mr. STEPHAN. That must have been an earlier version of the BZPP for '06 process. I saw what I think is probably a similar version about 2 or 3 weeks ago; and I told my people that is not the way, in fact, we are going to do this. The BZPP thing, we have to take a look at using a risk-based approach. We are going to have to marry it up with the UASI program, marry it up with the transit grant programs. We are going to focus it where we have clusters of targets so we can get more bang for the buck.

Because the intent of this program is to drive operational planning between State and local governments and the private sector and help those people develop operational prevention and response capabilities clustered around key areas where nuclear plants, chemical plants, transportation systems—where if we are going to provide grants to law enforcement capability, it can surge multiple ways.

That is one piece of this, but there are still important facilities across the country that may not be clustered with others, that are standalone, very consequential; and the BZPP program has to take those into account. I think one of the Secretary's visions in creating this new preparedness directorate, of which IP would be a part as well as the new Assistant Secretary for Grants in Training, is to make sure we are logically looking at what the requirements are across the board, figuring out what the criteria are for the different individual grant programs and making sure we are putting the most bang for the buck where it makes sense based on risk.

Mr. LUNGREN. I am going to recognize the gentleman from New Mexico but first mention, at least from what I hear at the local level in my State, what you have just said has not been conveyed to them. Somehow it was conveyed to them every State was going to get a predetermined number of slots, irrespective of risk; and the States would decide what they do. The number we heard was 70 to each State, and that didn't seem to me to make a whole lot of sense.

Mr. Pearce is recognized for at least about 5 minutes.

Mr. PEARCE. Thank you, Mr. Chairman.

If we explore this risk-based prioritization again as Secretary Chertoff has placed emphasis on, can you—what is the ultimate determinative risk?

Mr. STEPHAN. There are three pieces to the risk puzzle.

The first piece is threat information, which, sadly, is not always as granular as we would like it to be with respect to these critical infrastructure, key resource sectors, although we are following it

with very smart people every single day. Just never seems to get us the granularity expect for some specific instances you all know about, mainly in the mass transit world over the last several months.

The other piece of the equation is consequences, consequences in terms of public health and safety, human lives, human impacts, economic consequences, national security consequences. Those go into the mix.

And, finally, vulnerabilities, just how vulnerable is a consequential facility with respect to various potential modes of terrorist attack.

All of these pieces involve a formula that is basically consequences times vulnerabilities times threat equals risk.

Mr. PEARCE. So if we were going to say look at the nuclear power plant that is just west of our State in eastern Arizona and we are going to assess the risk of that versus a conventional power plant located in New York State with a dense population, which of those is going to percolate higher in the risk stream?

Mr. STEPHAN. If you go strictly by consequences in terms of population impact, naturally the piece in New York is going to receive more attention. But I also have to say this is not—this is an art, this is not a science; and I would say a successful attack on any nuclear plant anywhere in the United States of America is going to have a very important psychological dimension that no mathematical formula can bring to the table.

So in addition to those pieces of the risk calculus, we have to have good old-fashioned common sense and roll in some Kentucky windage reference psychological impacts to all of these target sets out there.

Mr. PEARCE. I understand that, but as a Department agency and looking at Secretary Chertoff's emphasis on risk-based prioritization, I am just asking which is going to percolate higher in the stream.

Mr. STEPHAN. I think all nuclear power plants are going to receive a high priority focus across the country.

Mr. PEARCE. If we then downgrade the risk to the next level and we look at water systems and you get, say, a water system pretty well protected and not very vulnerable, no threat info, and you have the open lake in New Mexico that feeds all down through Mexico and Texas, through the rest of New Mexico, and a biological hazard placed in that, no threat info on that, so which of those are going to percolate to the higher end of the risk-based assessment?

Mr. STEPHAN. Again, then we get a little bit more into the mathematical calculus piece. But this is not a winner-take-all or a winner-loser zero sum game. No matter what your level of risk happens to be, there are certain kinds of things that the Department of Homeland Security is going to reach out and touch you on. Everyone is going to be part of some kind of organized leadership structure that allows us to interact and interoperate and figure out what each other's needs and requirements are.

Everybody that wants to be is going to be tied into an Information Sharing Mechanism, no matter what your level of risk, because I hope to God in all this risk-management piece that al-Qa'ida kind of follows our own risk-management methodology or we

could be in trouble. Therefore, everybody—if you are on a target set today that meets our risk criteria, but al-Qa'ida goes another way, everybody has to be connected from an information perspective so we can rapidly adjust from where we think they hit us to where they might hit us based upon their own calculations.

So when we say risk-based focus, I am really talking about an allocation of DHS dollars and specifically IP dollars in terms of the monies we have at our disposal for specifically targeted initiatives like BZPPs, or buffer zone protection plans. Everybody is going to get a leadership structure put on top of them that they participate in. Everybody is going to get an information-sharing mechanism. Everybody is going to get access to a widely accepted vulnerability assessment methodology set of criteria and tools to help them out. And everyone is going to get information bulletins that specify specific threats when they do arise.

So I don't want to leave you all with the impression this is a zero sum game in terms of risk. There are certain baseline things everyone will be plugged into or be a part of.

Mr. PEARCE. Being from one of the rural areas, I will tell you that the great concern is that, through whatever mechanism that bureaucracies work and agencies work, is that risk-based is going to end up percolating down to population; and I will tell you that the Nation will be worse off than better off if population becomes a single criteria. I know you are telling me that is not the case, but I will tell you that human nature is that we try to find the easiest solution when the solutions are not very easy.

I will tell you that the nuclear components in New Mexico, with al-Qa'ida sitting there, coming across a border, that has nobody posted on it now. Last night, we got word that the border patrol has completely evacuated, and we are the last to learn that al-Qa'ida has come across our border. We get that in the newspapers when everybody else reads it. Somewhere we have to do a little bit more thorough job of understanding that risk-based is a little bit broader than just population. That I think is a task for us to remember through the long, dark nights of trying to assess our risk, but I appreciate your work on the effort.

I yield back.

Mr. STEPHAN. Thank you, sir.

Mr. LUNGREN. Colonel, if I could just ask you something with respect to an issue we dealt with on the committee yesterday that has to do with the Bureau of Reclamation.

They run over 400 dams and levee assets in the western half of the country in the 17 western States. They have what they would describe as a rather robust effort to provide security for their assets. Is your operation informed of their efforts? Are you integrated in any form, shape or fashion? What added value do you provide to them, if any, over and above what they are doing? And how does that contrast with what your other elements of DHS are doing with the other dams?

Because we are talking about 400 dams, levee assets under Bureau of Reclamation. That doesn't talk about State dams and certainly doesn't talk about privately owned dams.

Mr. STEPHAN. Yes, sir. Our problem is we have about 80,000 or so dam structures and levee structures across the United States of

America. I think about 5 percent may be owned by the Federal government across multiple agencies. The rest are State and local owned and operated facilities.

Our value in this has given this incredible patchwork of ownership authorities, regulations, resource dollars that go into this, is to provide an organizing leadership to all of that patchwork of different people out there searching for leadership. Through the NIPP structure, the National Infrastructure Protection Plan organizing umbrella, we at DHS IP lead the dams sector in terms of the government coordinating council represented by DOI, the Bureau of Reclamation, the Army Corps of Engineers, Agriculture, Energy, the Department of Defense, other folks that own dams wearing Federal hats. We also, through that coordinating council, bring together the major State players that own dams within their jurisdictions; and we have a private sector and some State membership on another council that we also bring to the table so that all of those equities are there. Our goal is to bring this amazing patchwork of different dam owners and operators together, make very sure that all those people are connected to some kind of information-sharing network.

The Federal pieces of the puzzle are fairly well connected together at this point in time. The State pieces of the puzzle are connected very well through the homeland security advisor network at this point. We have more work to do in terms of connecting individual State-level and private-sector dam owners and operators together from an information-sharing piece. Right now, we reach out and touch them through local law enforcement networks in partnership with the FBI, but I also need to be able to reach out and touch the owners and operators of those various facilities together.

We work together, realizing that some people like Bureau of Reclamation has some important resources they can bring to the fight. In other cases, where there is nobody covering down on a particular set of assets, we may make a buffer zone protection grant available based on consequences to a State government that has an important dam within its jurisdiction and try to make all of that work in some meaningful way.

Again, just a lot of different actors out there, a lot of players, a lot of information needs to be shared. We have to work together to make sure we clearly have identified what is more important than other things based mainly on consequences in the dams world and that we are all putting some kind of resource patchwork together to get at the really significant problems.

Mr. LUNGREN. I hope you don't mind if I harp a little bit on dams, but as I have explained before, I live downstream of a major dam that has been identified by the Bureau of Reclamation as one of concern.

Let me ask you about this. DHS and with dams, other than this information sharing and trying to get people together and so forth, do you have any operational responsibility in a terrorist attack scenario? What I mean by that is this—We know now, because we have had a couple of breaches of the no-fly zone around the D.C. area, that there is a decisionmaker that makes the decision as to whether or not to shoot down a plane. What about in terms of critical assets like a Federal dam?

I am not going to talk about any specific dam, but dams have different structures. You may have a reservoir that has several dams on it, maybe earthen, maybe the concrete structure, maybe dikes. A determination could be made at a particular time that, because of a threat to it, they have to relieve some stress on certain areas; and that decision could put some population centers at risk more than other population centers, actually, life-and-death situations.

Do those decisions that would be made operationally by Bureau of Reclamation in that context, would they in any way interface with the Department of Homeland Security before that decision is made or is that decision made within the Bureau itself?

Mr. STEPHAN. Sir, again, the decisionmaking power, as you correctly stated, resides with those organizations. But I think if we are talking about a terrorist incident here in terms of prevention, protection, response and recovery phases, DHS owns the overall operational coordination piece across the Federal Government for each particular phase of a response to a potential terrorist threat or national incident. There is an important role that headquarters would play in terms of that operational information-sharing reference the threat, reference protective measures that are in place and that need to be bolstered through the State homeland security advisor network principally as well as our Federal Department and agencies if it is a Federal asset.

The FEMA component of DHS has a very significant role to play in terms of consultation and the emergency preparedness posture of the downstream communities. There is a big program in FEMA, the Dams Safety and Security Program, that was created back, I think, in 2002 by an act of Congress that give those guys some very specific roles and responsibilities and some grants to facilitate preparedness planning on a steady state basis every day of the year, as well as technical assistance, as well as some other security-related activities.

Mr. LUNGREN. Maybe I will have to follow up with you at some other time, and maybe I need to look at some of the tabletop exercises that have gone on. It just strikes me after seeing Katrina and some suggestion that we didn't have—we had failure of decision making in some areas and not others. And posse comitatus, that goes in there. But if you have got a Federal facility and a terrorist attack, I don't think you have to worry about posse comitatus, but I think it would be good for us to insure we know what the chain of command is and the decisionmaking, where it may be considered operational of a dam or other asset. But the decision could very well determine who is in harm's way by the election of the decisionmaker, and I just would hope that we think about that ahead of time.

Mr. Pearce, if you have some further questions.

Mr. PEARCE. I do, Mr. Chairman, one more series of questions.

Mr. Stephan, the idea that we have got 80,000 dams out there that need some sort of protection plan, is homeland security going to provide the protection plan for each one of those?

Mr. STEPHAN. No, sir, we are not. The protection plan is the responsibility of the owners and operators.

Mr. PEARCE. How can we tell when they have done their homework?

Mr. STEPHAN. That is the challenge. There is no way that we can insure that 80,000 facilities—and they go from things like the Grand Cooley dam all the way to a simple earthen levee that is part of some neighborhood complex.

Mr. PEARCE. Early on, our office engaged in the difficulty of not only dams—I mean, 80,000 dams tends to put it in perspective, but if we look at the number of communities with the number of risks in communities, there is no way the Federal Government can identify and understand each risk, that it becomes a local and a State responsibility but mostly it is a local responsibility.

In trying to put some sense into that process, our office early on established—we went to one of the institutions that is syndicated with several other higher education institutions to provide security for the Nation and security training; and they helped us develop a thing called Certified Communities, with 35, 34 different components that are measurable—many are already measured, just not tabulated—and we created a concept called Certified Communities.

The idea is that the certified communities would get some sort of rating from insurance agencies. The insurance agencies do that right now, the ISO ratings for fire. What happens if your community loses its capability or drops its training for fire protection, homeowners get increases in their insurance policies. So what you have is you have all the residents of a community become kind of overseers. They are the first to realize that their insurance rates are going up because our community has not prepared itself. And if our community hasn't prepared itself then they call and they begin to raise pressure, you guys have let your ISO rating drop and we now are paying more insurance.

So it is not just that you need a program but you need a program that reinforces itself, that self-enforces it; and tying it to insurance rates is a way to get the public vision on it.

The second aspect of tying it to that is communities will know, if they have a better ISO rating, then their personal insurance costs go down. So, many times, they can pay for the protection that they are getting through the lower insurance premiums for the community.

Now we submitted this thing, and it has been locked down in ODP for about 6 months, and they refuse to bring it to the light of day. We think it could be done regulatorily, and it just does not make sense that Homeland Security has got this thing deep-sixed. It is just a gift that these education institutions have given to the Homeland Security Department. It would be very easy to implement, and it doesn't have any requirement that you do it. It just gives us a measuring stick, gives the tie-together that if you do—we visited with the insurance industry. Would you be willing to give better rates if communities are prepared against either terrorist threats or natural disasters, and they said of course we would.

So the enforcement mechanism is right there. That is the people and their insurance accounts. I just—someday maybe Homeland Security is going to think it important enough to get those 80,000 dams certified and all the communities across the Nation, some sort of process to where people will know if they are actually doing their work to prepare or not. It is very frustrating from our point

of view to have asked agencies or institutions to do this of work and then have it locked down over in ODP. So if you want to make a comment, fine.

Mr. STEPHAN. The only comment, I am not aware of the status of this paperwork, but I will go back and press on that.

Mr. PEARCE. I would appreciate it. It just makes sense for the Nation and appears like it would give us a measurement mechanism. The thought process that went into it came far broader than just into New Mexico. It was institutions across the country that are in this group that just worked to prepare.

Mr. STEPHAN. May I ask for the title of the program?

Mr. PEARCE. Certified Communities Program.

Mr. STEPHAN. Certified Communities Program.

Mr. PEARCE. It is very straightforward.

I appreciate it, Mr. Chairman. Thanks for your indulgence.

Mr. LUNGREN. I thank the gentleman from New Mexico for his questions, his inspiration and his persistence. I thank the witnesses for their valuable testimony and the members for their questions. I just want to let you know the absence of more members is not an indication of an absence in the interest of the work that you are doing, but it is the fact that at 12:30 we stopped having votes.

Mr. PEARCE. The other people got their airplanes out, and we did not.

Mr. LUNGREN. Mr. Pearce and I decided we would rather stay here with you.

The members of the Committee, as you know, may have some additional questions for you, and some will be submitted to you in writing. We would ask for you to respond to these in writing in a timely fashion. The hearing record will be held open for 10 days.

The subcommittee stands adjourned.

[Whereupon, at 4:27 p.m., the subcommittee was adjourned.]

FOR THE RECORD

PREPARED STATEMENT OF THE HONORABLE KIP HAWLEY

SPETEMBER 7, 2005

Good morning, Mr. Chairman, Congresswoman Sanchez, and Members of the Subcommittee. I am pleased to have this opportunity to testify on the subject of protecting civilian targets from terrorist attack. My focus today will be on the programs and initiatives of the Transportation Security Administration (TSA) in rail and mass transit security—where we are investing our resources and why—as well as our immediate response to the London bombings and our vision for the road ahead.

TSA is an agency created on the heels of the atrocious 9/11 attacks on our Nation. We are charged with protecting all modes of transportation—a mandate we have taken seriously since our inception, notwithstanding the more visible comprehensive federalization of our Nation's aviation security system directed by the Aviation and Transportation Security Act (ATSA). The tragic bombings in Moscow on February 6, 2004, in Madrid on March 11, 2004, and in London on July 7, 2005, and the attempted attacks there two weeks later, are grim reminders of the heinous tactics of our enemies and of the need to remain vigilant and prepared.

Our Current Program

Efforts to ensure transportation security vary with the nature of the system being protected. The Nation's rail and mass transit systems are fundamentally different from our aviation system. Transportation systems differ in size, in openness, and in control. Most importantly, our passenger rail and mass transit systems are, by design, far more accessible than the commercial passenger aviation system, with multiple entry points, few barriers to access, and hubs that serve and allow transfers among multiple modes—subway, intercity rail, commuter rail, and bus—and multiple carriers. While commercial passenger aviation is a closed system that can be closely monitored at controlled checkpoints, passenger rail and mass transit are open systems without controlled checkpoints—hence, monitoring cannot be accomplished by a single staff person or closed circuit television. Many passenger rail and mass transit systems are vast in terms of infrastructure and ridership. As just one example, each weekday an average of 4.5 million passengers ride the New York City subway, compared to approximately 1.8 million domestic aviation enplanements per day, *nationwide.* In addition, passenger rail and mass transportation assets are owned or controlled by State or local governmental entities or private industry, each of which is responsible for its own security. The Federal government has only very recently issued security regulations in mass transit and passenger rail. In contrast, although commercial passenger aviation also has a wide variety of owners and operators, its security has historically been heavily regulated by the Federal government.

And so, we cannot simply graft our commercial passenger aviation security systems onto the passenger rail and mass transit modes. To do so would be unrealistic, expensive, disruptive, and ultimately ineffective. Instead, we have, since our inception, been carefully weaving a web of security measures that depend upon three key components: stakeholder partnership and cooperation; risk assessment; and technology evaluation. These components have provided a strong security base and promise to strengthen mass transit and passenger rail security as we move forward.

Stakeholder Partnership and Cooperation. One hallmark of our rail and mass transit security program is the close working relationships we have fostered with other DHS components, with the Department of Transportation (DOT) and its modal administrations, and perhaps most importantly, with the stakeholders—the public and private providers of rail and mass transit transportation who are also responsible for the systems' security. Our efforts have focused on greater information sharing between the industry and all levels of government; addressing vulnerabilities in the rail and mass transit sector to develop new security measures and plans; increasing training and public awareness campaigns; and providing greater assistance and funding for rail and mass transit activities.

Risk Assessment. Security measures are a filter, not a guarantee, but effectiveness can be maximized, without unduly sacrificing freedom of movement, through risk assessment. A primary goal of our approach to security is to assess the risks and evaluate vulnerabilities associated with different components of the rail and mass transit systems to determine how to optimize resources. TSA's initiatives are intended to focus the collective limited resources available on the protection and prevention of terrorist incidents with the greatest potential consequences.

Technology Evaluation. The challenge of harnessing security technology for rail and mass transit is two-fold: How can we best adapt the security technology developed for aviation to the unique circumstances of rail and mass transit systems? What new technologies are uniquely suited to rail and mass transit systems? Pilot programs, exercises, and research and development aim to leverage current and emerging technologies to deter attacks against rail and mass transit systems, especially those intended to cause catastrophic damage through use of chemical, biological, radiological, or high explosives weapons.

Together, these three components support our current security program and future planning.

Grants. Although primary responsibility for funding mass transit security rests with State and local governments, substantial Federal assistance has been and will continue to be provided through a variety of grants. TSA has worked closely with DHS' Office of State and Local Government Coordination and Preparedness (OSLGCP) in the review of grant applications, the determination of eligibility, and final award determinations. Since its creation, through the State Homeland Security Grant Program and the Urban Area Security Initiative, DHS has allocated $8.6 billion for counterterrorism preparedness. The President's FY 2006 homeland security budget proposes an additional $2.4 billion for this purpose as well. These funds can also be allocated by State and local governments for rail and mass transit security efforts. The FY2006 budget also requests $600 million—a more than 60 percent increase—for the Targeted Infrastructure Protection Program, which covers security for mass transit, rail, ports, inter-city buses, and programs such as highway watch and buffer zone protection. These areas and programs combined received $365 million in FY 2005. Additionally, to date DHS' Transit Security Grant Program (TSGP) has provided more than $255 million to State and local transit authorities to increase protection through hardening of assets, greater police presence during high alerts, additional detection and surveillance equipment, increased inspections, and expanded use of explosives detection canine teams. In April 2005, DHS announced $141 million in TSGP funding, of which more than $107 million has been dedicated to owners and operators of rail systems. An additional $6 million was awarded to Amtrak through the Intercity Passenger Rail Security Program for security enhancements to rail operations on the Northeast Corridor and at the railroad's hub in Chicago.

TSA has also coordinated closely with DOT's Federal Transit Administration (FTA), which launched a comprehensive public transportation security initiatives program funded primarily through a $23.5 million supplemental security allocation in an FY 2003 emergency wartime appropriation. The program included threat and vulnerability assessments at 37 of the largest transit agencies, most involving multiple modes; the deployment of on-site security technical assistance teams to the 50 largest transit agencies; the award of security drill and exercise grants to over 80 transit agencies; the launching, with industry partners, of a Transit Watch security public awareness campaign; and the development and holding of community forums to enhance coordination and integration of transit agencies with emergency responders, fire and police departments, and other key stakeholders.

Security Exercises and Training. TSA has held numerous security exercises that bring together rail carriers, Federal, State, and local first responders, and security experts to test preparedness and response and identify best practices and lessons learned. These efforts support effective relationships among Federal entities and with State and local governments and the private sector and greatly enhance our overall security posture. These exercises assist TSA and stakeholders in addressing gaps in antiterrorism and response training among rail personnel.

Through an interagency agreement with the Federal Law Enforcement Training Center, TSA has trained over 400 law enforcement, transit police, and first responders through the Land Transportation Anti-Terrorism Training Program. Additionally, TSA has contracted with the National Transit Institute to develop a CD–ROM based interactive training program for passenger and freight rail employees. This product is expected to be completed before the end of the current fiscal year.

Stakeholder Engagement. TSA has reached out and engaged with industry stakeholders, including the American Public Transportation Association and Amtrak, to identify common security practices and obtain feedback on security programs and initiatives. This input is crucial to TSA's efforts to identify best practices, which will enhance security in the rail and mass transit modes. We are committed to maintaining these engagements and using the information and experience gained in security measures and programs.

Corporate Security Reviews (CSR). Since FY 2003, TSA has conducted 27 on-site corporate security reviews with rail and mass transit stakeholders, including six of the Nation's seven Class I railroads, to gain an understanding of each surface trans-

portation owner/operator's ability to protect its critical assets. The program's goals are to supply baseline data that can be used to develop security standards, provide domain awareness of security measures throughout the transportation sector, and promote outreach to transportation stakeholders as a means to ensure constant communication and foster stakeholder relationships.

The CSR Program has several recognized benefits. The data collected during these visits, such as security plans and critical infrastructure lists, supplies TSA with information to assist with other programs and exercises, baseline the state of security in the Nation, and establish performance-based security standards. This data also assists TSA in identifying areas where additional resources need to be dedicated to address security shortfalls. Additionally, the field presence fosters a higher degree of confidence in TSA with the stakeholder community, builds trusted partnerships faster, and validates stakeholder policies and procedures already in place.

Security Directives. To secure the U.S. passenger rail and mass transit sectors after the Madrid attacks, TSA issued Security Directives (SDs) that mandate specific security measures. The SDs set a standardized security baseline. They were developed in conjunction with stakeholders and DOT. The measures required by the SDs support DHS's overarching goals of prevent, protect, respond, and restore. A key measure mandated by the SDs is frequent inspections of key facilities, including stations, terminals, and passenger rail cars, for suspicious or unattended items.

Surface Transportation Inspection Program. In addition to the grant programs I have discussed, the Department of Homeland Security Appropriations Act for FY 2005 committed $12 million to TSA for rail security, including $10 million to deploy 100 Federal security compliance inspectors. TSA has made substantial progress in developing a robust and comprehensive surface transportation security compliance inspector program with emphasis on hiring, training, and logistical and procedural planning. More than 60 have been deployed to date. TSA expects to have hired and deployed all 100 inspectors to field locations in the next 60 days. The inspectors will identify gaps in security and inspect for compliance with the SDs.

Pilot Programs. TSA has successfully conducted the Transit and Rail Inspection Pilot (TRIP) program, which was designed to test the feasibility of screening passengers, their luggage, and cargo for explosives in the rail environment. The pilot occurred in three phases and tested advanced automated x-ray explosives detection equipment and canine patrols. TRIP provided valuable lessons on how to successfully deploy, maintain, and use screening technology outside the airport environment. Results indicated that such technology might be useful if threats were made against a specific rail or mass transit system or in support of a National Special Security Event (NSSE). This aspect was successfully demonstrated at the Republican National Convention in the summer of 2004 and at the Presidential Inauguration in January 2005.

Explosives Detection Canine Teams. The FY 2005 DHS Appropriations Act also includes $2 million to deploy explosives detection canine teams. The National Explosives Detection Canine Team Program consists of two components. First, a Rapid Deployment Force (RDF) has been developed to deploy DHS explosives detection canine team resources in support of local law enforcement agencies on an as needed basis in the event of heightened levels of security. TSA's participation in the RDF has included augmentation of local law enforcement and local authorities during NSSEs, such as the Presidential Inauguration and the Democratic and Republican National Conventions, as well as conducting joint training and assistance to existing mass transit canine teams. The second component of the explosives detection canine team program is devoted to rail and mass transit and should be completed by the end of calendar year 2005. This segment is being accomplished by partnering with local mass transit and rail authorities. It includes the training and deployment of additional TSA-certified explosives detection canine team assets to support mass transit systems and the development of national standard operating procedures for rail and mass transit systems. As one example, TSA partnered with the Metropolitan Atlanta Rapid Transit Authority, deploying six TSA-certified explosives detection canine teams throughout their system.

This program is effective and expanding. On August 10, 2005, TSA offered a cadre of three dogs each to ten of the largest mass transit systems in the Nation. Law enforcement officers from the ten systems that choose to participate will attend the TSA Explosives Detection Canine Handler Course beginning this month. During that ten-week course, handlers will be matched with a TSA canine and trained in proper dog handling and search techniques. Upon graduation, the teams will return to their systems for local training, familiarization, and certification.

Hazardous Materials. The security of hazardous materials (HAZMAT) shipments, including radioactive materials and defense related items, is an area that has received special emphasis since September 11, 2001. DHS and DOT have been work-

ing on several initiatives that support the development of a national risk-based plan to address the shipment of HAZMAT by rail and truck. For rail, a major effort is the assessment of the vulnerabilities of urban areas through which toxic inhalation hazard (TIH) materials are transported. TSA and DHS' Directorate for Information Analysis and Infrastructure Protection (IAIP) have worked together to enhance security in the Nation's capital with the National Capital Region (NCR) Rail Security Corridor Pilot Project. The $9.6 million pilot initiative established a seven-mile long Rail Protective Measures Study Zone to protect HAZMAT traveling through the city. Measures undergoing testing and development include screening and monitoring of trains, monitoring of personnel, chemical monitoring, radiation and contamination monitoring, and physical security measures to prevent intruders from tampering with the rail lines or trains. The task force for this effort includes private stakeholders and other Federal and local government agencies that conducted risk vulnerability assessments and identified critical areas and mitigation strategies to enhance HAZMAT security along the D.C. Rail Corridor.

TSA continues to improve HAZMAT security through the High Threat Urban Areas (HTUAs) Corridor Assessments. The DHS/DOT team is conducting vulnerability assessments of HTUAs where TIH HAZMAT is transported by rail in significant quantities. TSA, IAIP and federal partners from DOT (Federal Railroad Administration (FRA) and Pipeline and Hazardous Materials Safety Administration (PHMSA)) have completed four corridors. The goal of DHS is to complete nine corridor assessments of selected high-threat urban areas by the end of this calendar year. These assessments comprise one portion of a DHS and DOT plan to enhance the security of TIH rail shipments. Other goals of the plan are to enhance the ability of railcars to withstand attack, improve compliance with security plan regulations, develop protocols for protective measures, establish communication standards on rail car tracking systems, and improve rail car security during storage in transit.

TSA contracted with the Texas Transportation Institute (TTI) to conduct an independent rail HAZMAT placarding study to assess the feasibility of technological alternatives to the current placard system that would enhance security while maintaining the same level of safety for the first responder community. TTI identified alternatives in three categories: cloaking devices; decentralized systems; and centralized systems. The study was completed on December 17, 2004, but the technologies examined did not demonstrate capabilities that would justify replacing the current system. Therefore, the Secretary of Homeland Security has decided that the current placarding system will remain in effect.

In addition, FRA has administered and enforced the hazardous material shipment regulations promulgated by PHMSA or its predecessor, DOT's Research and Special Programs Administration since the 1970s. These safety regulations cover multiple subjects implicated by the shipment of HAZMAT by rail, including loading, unloading, transloading, placarding, rail car placement in trains, and documentation of the movement. There are nearly 100 FRA and State inspectors involved in aggressively inspecting and enforcing the HAZMAT regulations with respect to railroads, shippers by rail, tank car manufacturers, and tank car repair facilities. The FY 2005 FRA budget provides funding specifically for additional HAZMAT inspectors for tank car design, construction, quality, and maintenance.

Freight Rail Security Demonstration Projects. TSA has worked with IAIP and DOT's FRA and PHMSA to develop projects to be funded with $5 million allotted from the appropriation in the FY 2005 DHS Appropriations Act to OSLGCP for intercity passenger rail transportation, freight rail, and transit security grants. These projects will be carried out in accordance with the September 2004 Memorandum of Understanding between DHS and DOT on agreed upon roles and responsibilities. Through this team approach, OSLGCP, TSA, IAIP, FRA, and PHMSA will engage stakeholders at the ground level in designing a comprehensive and meaningful strategy for successful implementation of the proposed demonstration projects.

Self-Assessment Tool. TSA has developed a Vulnerability Identification Self-Assessment Tool (VISAT), a multi-modal tool that a rail or mass transit system may voluntarily use to detect and weigh the vulnerabilities within their systems. In general, the tool focuses on the prevention and the mitigation of an array of threat scenarios developed for each mode within the sector. Users rate their entity in terms of target attractiveness (from a terrorist's perspective) and several consequence categories that broadly describe health and well-being, economic consequence, and symbolic value of the entity. The tool enables a user to capture a snapshot of its security system baseline by assessing vulnerabilities in the system and assisting in the development of a comprehensive security plan.

Of note, VISAT has been adapted for use by stadium and arena managers to enhance security as well. To date, access to VISAT has been provided to over 300 stadiums and 400 arenas. IAIP is spearheading efforts to adapt the program for use

by other commercial sector venues, to include convention and performing arts centers. An IAIP pilot program with the States of Texas, Virginia, and California, aims to adapt the tool to support security awareness in K–12 schools.

Infrastructure Protection. TSA has been integral in assessing the vulnerability of rail and mass transit infrastructure. To date, TSA has reviewed over 2,600 facilities, structures, and systems in a comprehensive effort to determine critical infrastructure. DHS has conducted 52 Site Assistant Visits (SAVs) in the transportation sector including mass transit systems, tunnels, bus terminals/systems, rail lines, and bridges as of August 26, 2005. DHS and TSA personnel continue to review the security plans, countermeasures, mitigation strategies, and technologies used by industry, and will identify best practices in the future.

FRA is assisting Amtrak in enhancing the security and safety of New York City tunnels under the East and Hudson Rivers. TSA and FTA are assessing the security of high-risk transit assets, including vulnerabilities in subway tunnels and at stations where large numbers of people converge and where an attack would cause the greatest loss of life and disruption to transportation services. FTA is working with local systems to develop best practices to improve communication systems and develop emergency response plans.

By a final rule issued on May 31, 2005, FTA met Congressional direction to establish a program providing for State-conducted oversight of the safety and security of rail systems not regulated by FRA. To be codified at 49 C.F.R. Part 659, the rule imposes specific requirements for the development, implementation, monitoring, and assessment of security plans in addition to expanding safety oversight requirements.

Response to the London Attacks

The recent London subway and bus attacks reaffirmed our need for vigilance in securing our rail and mass transit systems. The nationwide response to those attacks, however, also affirms the capability of TSA's approach to mass transit security to date. TSA and FTA jointly surveyed the top 30 transit agencies to determine changes in their security posture. Even before DHS officially raised the threat level for this sector, many transit agencies had voluntarily enhanced their security with additional patrols, explosives detection canine support, and enhanced public awareness campaigns. These efforts built upon improvements in the security posture brought on by adherence to the security directives TSA issued in the aftermath of the Moscow and Madrid bombings in 2004. Most transit agencies also increased the frequency of security inspections, including track inspections. Many indicated that they would continue increased use of these resources even after the downgrading of the threat level from Orange to Yellow.

In the immediate aftermath of the bombings, TSA personnel were given access to transit agencies' operations centers nationwide to observe and evaluate and assist in responsive measures. TSA's surface transportation inspectors deployed to the operations centers of the major railroads and transit systems across the Nation to assess security posture and facilitate protective actions. FRA safety inspectors provided exceptional support and assistance in this effort with the railroads. This collective effort leveraged the assets, expertise, and carefully fostered partnerships of government and industry stakeholders to increase our situational awareness. Lessons learned by all parties will enhance overall security posture and awareness and foster effective cooperation and partnering among Federal, State, local, and private sector entities in the prevention of, and response to, acts of terrorism.

Internationally, TSA officials have engaged with their foreign counterparts on rail and mass transit security issues, with the aim of sharing and gleaning best practices from countries with a history of terrorism against their surface transportation systems, an effort we will continue and expand upon. TSA has met with the responsible officials from the United Kingdom, Spain, Russia, Israel, France, Japan, Greece (particularly in preparation for the 2004 Olympic Games), the Netherlands, Canada, and other countries. TSA has developed forums for sharing security information and practices on behalf of DHS across all modes of transportation. TSA also benefits from the efforts of DHS representatives based overseas in U.S. Embassies, who have expanded their traditional aviation security roles to include security issues relating to all modes of transportation.

The Road Ahead

We go forward with a disciplined measured program for protecting our rail and mass transit systems. Our efforts will continue to emphasize the shared responsibility of the Federal government, State and local governments, industry, and academia. TSA will continually set the standard for excellence in transportation security through people, processes, and technology.

Crucial to our success as we move forward will be our ability to determine how to best invest our resources. As we continue with our risk assessments and pilot

programs, we must optimize our resources to assure that they are invested where they will give the most information or protection. We cannot and will not arbitrarily push money into security programs without an intelligent assessment of their utility.

Securing rail and mass transit systems must be a shared effort among Federal, State, and local governments and private stakeholders. Owners and operators are properly responsible for their own security. In mass transit, well-trained local law enforcement personnel understand the unique design characteristics and security challenges of their home town systems far better than anyone else. Success depends upon an effective partnership that builds on the strengths and resources that each level—Federal, State, and local—can offer and reflects the unique attributes and architecture of each system. To foster this effort, TSA has initiated a pilot program aimed at leveraging and networking information resources to ensure decision-makers at all levels have the tools they need to implement measures and take actions to deter and prevent terrorist actions.

Our challenge is great—to assure security and protect lives and property while maintaining the access and efficient movement that is essential to rail and mass transit systems. Stakeholder partnerships, information networks, development and leveraging of technology, using a risk-based approach to deployment of Federal resources, grants to foster innovation at the State and local level and in the private sector—through these means, we will continue to strengthen our base of security programs in a manner that ensures freedom of movement for people and commerce.

Thank you for the opportunity to appear this morning. TSA looks forward to a continuing dialogue with Congress on the issues of rail and mass transit security. I will be pleased to answer any questions you may have.

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

November 2, 2005

The Honorable Steven Pearce
U.S. House of Representatives
Washington, DC 20515

Dear Congressman Pearce:

This letter is in response to your request at the October 20, 2005 hearing of the Committee on Homeland Security's Emergency Preparedness and Science and Technology Subcommittee. You asked for additional information on the Department of Homeland Security's efforts to review and participate in the Certified Rural Community Emergency Preparedness and Action Program (CRCEPA).

Officials from DHS's Office of State and Local Government Coordination and Preparedness (SLGCP) met with New Mexico Institute of Mining and Technology and New Mexico Military Institute along with Rhett Skiles, your Senior Legislative Assistant, to discuss the proposal in June. During this meeting, SLGCP offered feedback and comments on their proposal. Since that meeting, we have not received any additional information or an update from the NMT and NMMI representatives.

DHS has done extensive work on the assessments and measurements associated with HSPD-8 and the National Preparedness Goal (NPG). Once published, the final NPG, and accompanying guidance materials, will allow the Federal governments, States and localities to assess their levels of preparedness. DHS is planning to continue with its efforts to work with state and local communities to ensure they have the proper mechanisms to assess and maintain capabilities, establish procedures for incident planning, train to those capabilities promote interoperability through exercises and collectively increase the level of preparedness across the nation.

We look forward to working with your state and local communities in their preparedness efforts. DHS is committed to ensure that the Federal government, state, local, tribal and private sector is prepared for and ready to respond to a terrorist incident or catastrophic natural disaster.

Sincerely,

RB Stephan

Robert B. Stephan
Assistant Secretary for Infrastructure Protection

○