S. Hrg. 109–481

AFTER THE LONDON ATTACKS: WHAT LESSONS HAVE BEEN LEARNED TO SECURE U.S. TRANSIT SYSTEMS?

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

SEPTEMBER 21, 2005

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE
24–238 PDF WASHINGTON : 2006

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

SUSAN M. COLLINS, Maine, *Chairman*

TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
NORM COLEMAN, Minnesota
TOM COBURN, Oklahoma
LINCOLN D. CHAFEE, Rhode Island
ROBERT F. BENNETT, Utah
PETE V. DOMENICI, New Mexico
JOHN W. WARNER, Virginia

JOSEPH I. LIEBERMAN, Connecticut
CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK DAYTON, Minnesota
FRANK LAUTENBERG, New Jersey
MARK PRYOR, Arkansas

MICHAEL D. BOPP, *Staff Director and Chief Counsel*
KATHLEEN L. KRANINGER, *Professional Staff Member*
JOYCE A. RECHTSCHAFFEN, *Minority Staff Director and Counsel*
JOSHUA A. LEVY, *Minority Counsel*
TRINA DRIESSNACK TYRER, *Chief Clerk*

CONTENTS

WITNESSES

WEDNESDAY, SEPTEMBER 21, 2005

ALPHABETICAL LIST OF WITNESSES

AFTER THE LONDON ATTACKS: WHAT LESSONS HAVE BEEN LEARNED TO SECURE U.S. TRANSIT SYSTEMS?

WEDNESDAY, SEPTEMBER 21, 2005

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:02 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Susan M. Collins, Chairman of the Committee, presiding.

Present: Senators Collins, Lieberman, Levin, Carper, and Lautenberg.

OPENING STATEMENT OF CHAIRMAN COLLINS

Chairman COLLINS. The Committee will come to order. Today this Committee will examine the security and preparedness of mass transit systems in the United States. I particularly appreciate the chief operating officer of the London Underground traveling across the Atlantic to be with us this morning. He will share the lessons learned from his experience in leading his agency's response to the terrible attacks in July in London.

I would like to thank our distinguished Ranking Member, Senator Lieberman, for his initiative in recommending this hearing and our other expert witnesses for their appearance here today.

I would also note that the American Public Transportation Association is hosting a meeting of security officials from a number of foreign transit agencies in Washington, and many of them have joined us at this hearing today. They represent a number of foreign countries, and we welcome them and look forward to hearing their views after the hearing.

On the morning of July 7, terrorists exploded three bombs on underground trains in central London. A fourth bomb destroyed a double-decker bus. Fifty-two innocent people were murdered in those attacks. More than 700 were injured. Exactly 2 weeks later, on July 21, another attack was launched during London's morning rush hour. Again, three trains and a bus were the targets. Fortunately, however, those bombs failed to detonate.

The attacks on London's mass transit have been described as a wake-up call to those responsible for the safety and security of our own mass transit systems, and they are not the first. They echo the alarms set off by earlier attacks on mass transit in Madrid, Moscow, Tokyo, Tel Aviv, and other cities around the world. In fact, the

National Counterterrorism Center database reveals that in 2004, there were more than 150 deadly terrorist attacks on mass transit worldwide.

Now that we have heard the alarm bells, it is time to act. In the jargon of counterterrorism, we often speak of soft targets. Soft targets are those locations and facilities that attract large numbers of people and that, by their very nature, must be open to easy public access, such as schools, shopping malls, hotels, restaurants, and sports arenas. The American mass transit system is among the softest of targets. Every year, according to the American Public Transportation Association, Americans take more than 9.6 billion trips on public transportation. Every weekday, approximately 6,000 public transit systems carry more than 14 million passengers. In less than a month's time, transit systems move more passengers than U.S. airlines transport in a year. Implementing security measures for these necessarily open systems is both a challenge and a responsibility borne by Federal, State, and local government officials, as well as private-sector owners and operators. Meeting this challenge requires a strategic vision and short- and long-term action plans developed among these parties, and it requires leadership from the Federal Government.

I look forward to hearing today from the Department of Homeland Security regarding the Federal strategy for helping to secure our Nation's mass transit systems. I am, however, disappointed that that strategy was initially classified, making access to it extremely difficult. In particular, I also question whether the Department may be focused too narrowly on aviation security at the expense of other modes of transportation. While it is understandable that after the September 11 attacks air security would command our immediate focus, I believe that it is now time to reassess priorities and evaluate our preparedness across all modes of public transportation.

The answer, of course, is not merely to invest more in mass transit security, but to invest it wisely, to adopt and expand strategies and tools that have proven successful elsewhere. From communications, surveillance equipment, sensors, and access control systems to planning, training, additional transit police, and increased public awareness, the techniques by which mass transit security can be improved are known and in use, as our witnesses will testify today. I welcome the testimony. We will hear how these techniques can be employed to harden a target that remains far too soft.

Senator Lieberman.

OPENING STATEMENT OF SENATOR LIEBERMAN

Senator LIEBERMAN. Thanks, Madam Chairman. Thanks for your opening statement and thank you very much for convening this hearing. This Committee has been quite engaged as the oversight committee of FEMA and the Department of Homeland Security in the aftermath of Hurricane Katrina. In fact, tomorrow we are holding a markup—I believe the first by a Senate Committee—to bring out emergency response legislation; that is, legislation that will assist the victims and their communities in their response and recovery to Hurricane Katrina. So I appreciate your decision to go ahead with this hearing as scheduled, and I think it reflects our shared

conclusion that our transit systems remain vulnerable to terrorist attack and that the terrorists who struck us on September 11 are not going to take a holiday or a grace period because we have been hit by Hurricane Katrina. They are out there, and we have to do everything we can, urgently, to increase our defense, our homeland defense of targets that are vulnerable and may be therefore attractive to terrorists.

Many of us have been concerned, as your opening statement suggests, Madam Chairman, since September 11 with the lack of an adequate response to the defense of our mass transit systems. As you said, it was understandable post-September 11 that we should focus first on aviation security, and quite appropriately so. But September 11 was a tragic wake-up call that should challenge us to better defend not just aviation, but other transit systems and other vulnerable parts of our society. The numbers here cry out, just as you said. The number I have—more than 14 million Americans ride our mass transit systems every day, as compared to 2 million people who fly on airplanes. That does not mean we should not do everything we can aggressively to protect the 2 million. It just means that we better not forget the 14 million, and the response—perhaps this is too simple, but it is one measure—is how much money we have spent since September 11 on aviation security on the one hand and mass transit security on the other. You will get some debate about these numbers depending on how you calculate them, but there seems to be agreement that we have spent at least $15 billion on aviation security since September 11 and that we have spent only $300 million on mass transit security. That cannot go on. We are inviting trouble if it does go on.

For about 3 years, some of us have been trying to get the Administration to issue a National Transit Security Plan. Last year, finally, in the intelligence reform legislation which came out of this Committee and was adopted in December, there was a legal requirement to do that. It was due on April 1. A lot of months went by, but finally, after April 1, the plan was issued. And, as Senator Collins has said, it was classified, preventing many of the stakeholders in our mass transit system, for whom the document was issued, from being able to use it. I am pleased that the Department, hopefully—at least in part in response to the request made by Senator Collins and me—has now agreed to permit the stakeholders to view the strategy, but we are still unable to discuss the content of the document here today without restriction.

I do want to discuss—with Mr. Hawley, particularly—the Federal Government's vision for transit security and transportation security generally in a way that is constructive and meaningful without compromising any of the restrictions established by the Department. So I guess I would say right here at the outset to you, Mr. Hawley, and as far as it relates to any others, but it is really to you, that if at any point during the hearing in response to a question I or any of the rest of us ask, but I will say it about myself, you believe that a full answer would require you to discuss information that cannot be discussed publicly, then please indicate so and limit your answers to that which you can discuss publicly. I will say for my part I have reviewed the strategy, but I remain concerned that within it there is not an adequate sense of priorities.

The vulnerabilities are listed in different areas of mass transit—but there is not a sense that I got of priorities about which of those vulnerabilities are most significant and, therefore, which we should focus most resources on most quickly.

Second, I share with you a general reaction, and want to ask you about it, that the plan continues to reflect an encouraging, proactive, aggressive, creative, comprehensive, can-do, must-do attitude toward aviation security, but it does not do the same with regard to mass transit. We understand, as Senator Collins said, that a lot of forms of mass transit are more open systems, harder to protect, but that is not a reason not to do a lot of things that are not being done now to push, if I can use an old metaphor, the security envelope here—it is probably not the appropriate one—to make sure we are doing everything we can, even allowing for the openness of the systems.

In that sense, our witnesses today, I think, can be extremely helpful, and I am very grateful that they are here. Chief Brown, Mr. Brown, comes with the experience, not just of the tragedy of the attacks in London in July, but of all that the London system does to deter such attacks, well beyond what is done in most of our transit systems today. Mr. Ron brings considerable experience from Israel, unfortunately having lived with the clear and constant danger of terrorist attack, in other methods that can be used to deter those attacks in open mass transit systems. I look forward to hearing from him. And then Chief Hanson, from the Metro Police Department, is in some sense the consumer and the front-line first preventer, not to mention first responder, in mass transit security. I want to ask her about how she thinks we in the Federal Government are doing in helping her do her job. Bottom-line, I have, and I know everybody on the Committee does, a real sense of urgency about doing a lot better than we have done in protecting the American people when they ride mass transit in this country, and I am confident that from this hearing will come some good ideas that we can use together to accomplish that very important national security goal.

Thank you, Madam Chairman.

Chairman COLLINS. Thank you, Senator.

I would now like to call upon a Committee member who takes mass transit every day and thus has a special interest in this topic and has had for some time.

Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thanks, Madam Chair, and thanks very much to you and Senator Lieberman for holding this hearing. This is one that strikes close to home for all the members of the Delaware congressional delegation, Senator Biden, Congressman Castle, and myself, because we do commute on almost a daily basis to Washington along with hundreds or thousands of people who ride not just Amtrak, but the MARC systems, the SEPTA systems, and others up and down the northeast corridor, so we much appreciate your holding this hearing.

I flew down to Charlotte, North Carolina, on Monday and was reminded again as I stood in line to go through security at Philadel-

phia International to take my shoes off and to go through the process that we have all become familiar with in the last couple of years, how much air travel has changed in the last 4 years. Those of us who work the kind of jobs we do, we do fly a whole lot. So we are especially mindful of that. I am sure a lot of folks in the audience are mindful of that, as well.

I think most of us agree that American air travelers are traveling with greater security and that some of the inconvenience we put up with is worth it. I feel safer. I hope others feel safer, as well. I noted before—I think in this Committee—that the bombings that we witnessed in the past year or so in Madrid and in London should have in a lot of ways been the same kind of wake-up call for us that September 11 has been on the air side. We have taken some steps to secure rail and transit systems since those two attacks, but I am telling you I am still not convinced that we have done everything that we can and should be doing to prevent a Madrid-style or a London-style bombing from occurring here close to home on our own shores. I am not suggesting that we take what we are doing at our airports and set up similar security systems in trains or bus stations. I am not interested in rushing into the Wilmington train station, taking off my shoes, and standing in line to go through screening devices any more than the other hundreds of thousands of people who take transit every day, but I think there are some things we can do, and hopefully as we come through today's hearing we will identify some of them.

I am pleased that we have finally given the Department of Homeland Security the money to distribute grants to rail and to transit systems to help them pay for some of the cost of additional security. It is my understanding that not very much of that money has been spent, and I am not sure why that is the case. We certainly hope to get some insights into that today. Since Amtrak and most transit agencies barely have enough money to operate from day to day, we probably ought to be putting up the money, and I am just curious as to why the money that we have appropriated has not gone out the door and actually been put to work. I am also pleased, though, that the Department of Homeland Security is spending money to train and deploy teams of rail inspectors and canine bomb-sniffing units.

Whenever I talk to security folks within Amtrak, they always say one of the best buys that we can get for our money is dogs, just to have dogs that are trained with folks who know how to handle them to check for bombs aboard trains. I think we do need more information, however, about how these assets are going to be deployed and how they fit into a strategy to harden our defenses against an attack on our rail and our transit systems quickly before another attack forces us to take additional action.

In closing, Madam Chairman and colleagues, I will just say that this is, I think, a very timely hearing and a topic that is worthy of our attention and has been for some time. There has been a lot of talk since the London bombings about whose job it is to do the brunt of the work to protect our Nation's rail and transit infrastructure—the operators in the private sector, State and local level, or the Federal Government? I agree with those who say that rail and transit security should be a shared responsibility, but if, God

forbid, there were an attack on an American subway system like the one that occurred in London, our constituents would demand that the Federal Government act decisively, and I hope that this hearing helps us flesh out at least a little bit more what the Federal role in transit security and rail security should be and speeds up our efforts to fulfill that role.

Thank you.

Chairman COLLINS. Thank you.

Senator Levin, we welcome you, as well.

OPENING STATEMENT OF SENATOR LEVIN

Senator LEVIN. Thank you, Madam Chairman, to you and Senator Lieberman as always for taking a leadership role in a very critical area. One of the issues that I am particularly interested in in the area of transit security, but frankly all security, is the development of technology that is capable of detecting explosives at a distance. If we can develop that technology so that we can identify explosives at a distance, we are going to be able to dramatically enhance our security everywhere. The technology does not yet exist, as far as I know, and yet we have—as Senator Carper mentioned—dogs that sniff explosive material. Explosive residues can be detected on people and on clothing, and we should be able, if there are enough resources invested, to develop a technology which can spot explosive devices at some distance, and that would be a huge breakthrough in the fight against terrorism. So I know that the Department of Homeland Security is developing and coordinating an effort to detect the presence of explosives at a distance. I emphasize at a distance. We already can detect them at a few inches or feet. We need to be able to detect them at many yards away.

We could have protected ourselves and other countries could have protected themselves against many of these explosions had we had this capability. I believe we put some additional funds in the budget this year to do that. I think we have gone from $22 million to $136 million for the High Explosives Countermeasures Office, but I would like to hear from Mr. Hawley and also our other witnesses if they have information on this subject as to what is the status of the efforts to research and develop a detection capability for high explosives at some distance.

I regret that I am going to have to leave, so I will not hear their answers, but my staff will tell me whether or not either or any of these witnesses have been able to shed some light on this question as to where are the investments being made; what is the time line; do we have any hoped-for breakthroughs that are on the horizon? If so, with luck, can we be deploying these kind of detection devices or a detection device within a matter of a year or two, or is it longer range than that? How many companies do we think and how many institutions—academic institutions, commercial companies—are involved? Is it a matter of a few or is it a matter of dozens or is a matter of hundreds looking for this capability? And from our witnesses from England, if they could also bring us up to date as to what England is doing in this area, as well, it would be helpful to me. Again, I only regret that I cannot stay to hear the answers, but it is a very important question I hope our witnesses might address.

Chairman COLLINS. Thank you, Senator.

I am pleased to welcome our first witness this morning, Edmund Hawley, the Assistant Secretary of Homeland Security for the Transportation Security Administration. This is the position for which the Committee confirmed him this past July. We are very pleased to welcome you back, and we look forward to hearing your testimony. Please proceed.

TESTIMONY OF EDMUND S. HAWLEY,[1] ASSISTANT SECRETARY OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. HAWLEY. Thank you. Good morning, Madam Chairman, Ranking Member Lieberman, and Members of the Committee. I appreciate the opportunity on behalf of the Transportation Security Administration (TSA) to discuss our efforts in partnership with others in the Federal, State, and local governments, as well as the private sector, to provide essential security in public transportation. As has already been noted, 2½ months ago, Londoners endured the ordeal of four nearly simultaneous suicide bombing attacks in the Underground system and a double-decker bus. Just 2 weeks later, another four attacks in the Underground were attempted.

This has been an opportunity for us to assess and enhance the level of security on our public transportation systems. Our review of that effort has provided valuable information on our security posture and insight into areas where improvements are needed. These learnings from London and insights from Secretary Chertoff's second-stage review form the basis of my testimony today. Earlier this month, the Department delivered to Congress the national strategy for transportation security that you have mentioned. This was prepared in cooperation with the Department of Transportation and outlines the Federal Government's approach in partnership with State, local and tribal governments and private industry to secure the U.S. transportation system from terrorist attacks and also to prepare the Nation by increasing our capacity to respond if an attack occurs. It describes how the Federal Government will manage transportation risks and discusses how the government will organize its resources to secure the transportation system.

To implement the strategy, it is clear that we must enhance our coordination of security initiatives and our communication among the Federal, State, and local governments and industry stakeholders. Two significant developments in this area have already occurred. On September 8, TSA, FTA, and DHS's Office of State and Local Government Coordination and Preparedness (SLGCP) completed the public transportation annex to the Memorandum of Understanding (MOU) between DHS and DOT. This agreement defines the roles and responsibilities of the Federal Government parties in public transportation security. Additionally, earlier this month, as a direct result from our learnings from London, TSA initiated a pilot program with participants from DHS, DOT, and FTA to re-think the way in which we communicate with stakeholders on

[1] The prepared statement of Mr. Hawley appears in the Appendix on page 37.

passenger rail and rail transit security issues. The objective of this program is for the Federal partners in passenger rail and rail transit security to coordinate ahead of time and speak with one voice to our stakeholders. This program will bolster passenger rail and rail transit security and provide the foundation for similar initiatives in other transportation modes.

We are also bringing improvements to explosive detection procedures. We are increasing our canine explosives detection capability and have taken steps to expand the deployment of teams to some of the largest mass transit systems. That effort is now under way. TSA's surface transportation inspection force is nearly fully fielded. Inspectors are already deployed and working to develop close liaison with mass transit and passenger rail operators. The inspectors provided timely services in the aftermath of the attacks on London, deploying to rail and mass transit operation centers throughout the Nation. The lessons learned and relationships developed will further enhance our security posture, as will the security system evaluations in mass transit systems. These initiatives are being integrated into the broader context of overall DHS initiatives and Secretary Chertoff's strategy for the Department. These include real stakeholder engagement, networked information, development and leveraging of technology, a risk-based approach to the deployment of Federal resources, and the DHS program for grants to foster innovation at the State and local level and in the private sector. We will continuously strengthen our base of security programs in a manner that ensures freedom of movement for people and commerce.

A common theme in this discussion is our effectiveness and security depends on the close working relationships among the parties. I would like to publicly express my gratitude to Transportation Secretary Norman Mineta for his support of this mission by letting us take a key member of his team, Deputy Transit Administrator Robert Jamison, who will join us at TSA as deputy administrator. He brings a wealth of experience in the public transportation environment and is acting administrator of the Federal Rail Administration.

Thank you for the opportunity to appear this morning. I look forward to working with Congress on these topics and would be happy to answer any questions.

Chairman COLLINS. Thank you for your statement. I want to begin my questioning today by exploring an issue that Senator Lieberman raised in his opening statement about the disparity in funding for aviation security versus other modes of transportation. My statistics are a little bit different from those of Senator Lieberman, but the point is exactly the same. Since September 11, 2001, the Department of Homeland Security has allocated over $18 billion in funding for aviation security and only $250 million for transit security grants. Now, I recognize that the funding for transit security grants does not represent all spending that benefits transit security, but it is the largest allocation of dedicated funding, and by any measure there is a huge disparity. At this stage and in light of the attacks on mass transit systems in other countries, should we be reallocating resources to beef up other modes of transportation?

Mr. HAWLEY. The risk-based approach looks at the total transportation network, and clearly the Federal dollars that are spent in the aviation sector are very much larger than those spent in others. However, that does not reflect the relative importance of either the modes or the security available to them, and that it is a very high priority certainly in the Department and TSA to be involved in transit security. The numbers—there are a lot of different numbers, but I think your point is valid, whatever the specific numbers. But the way we look at the terrorist situation today is more on a person-based as opposed to a thing-based, which is to say that it is not, in our opinion, the right way to structure the security regime to look at specific attack points and develop solutions for every one of those individually, but rather to look at the whole system and say it is the people who are delivering these attacks, and things that we do in terms of border security, connecting the dots, so to speak, between ICE and Customs and border protection and TSA and FBI, and that the focus of finding the terrorists themselves who may decide to do a transit attack or an aviation attack or any of the other modes, that the focus is to stop the terrorist attack wherever it is, and certainly there are prudent things to do at the point of attack across the board, but there is also the other effort that does not lend itself to modal differentiation.

Chairman COLLINS. I think that is something that the Department really needs to take a look at. The GAO has been critical of the Department, as you know, for not concluding a risk assessment of the Nation's passenger rail system. And, there continues to be criticism of whether or not we are really prepared in this area. I also think we can learn a lot from the experience of other countries. In Michael Brown's testimony, he notes the value of the closed-circuit television surveillance units that are widely deployed throughout the London Underground system, and it was those television images that enabled a swift, successful law enforcement investigation following the July attacks. What is the status in the United States of efforts to install similar surveillance and communication systems within our mass transit systems?

Mr. HAWLEY. The camera systems and the communication systems are among the best security measures that the transit systems can do, and, of course, each system has its own particular characteristics and its own particular progress. The point that I always come to on that is that the capital expense of getting the camera installed is perhaps the easiest part, and then comes the part of, OK, how are we actually going to use them? Who is going to be watching the feeds? How are we going to analyze them, and what do we do when we see something that we are concerned about? From my point of view, as these issues are resolved on the capital dollars to put in these very excellent systems, that there needs to be a commensurate activity that integrates those new systems into the real world security process of an individual transit system or even transit station. So it is something that we feel is very important and a role that we can play that is helpful and directly applicable to increased security, but does not have a huge dollar cost associated with it. It is how to leverage those capital investments to get the best operating security.

Chairman COLLINS. Are other countries ahead of us in this regard? It certainly seems that way, just watching the images on television versus our personal observations here in the United States.

Mr. HAWLEY. Well, certainly the London Underground is among the best, if not the best in the world, in terms of the deployment of an integrated security system, and it is a cautionary tale that even with that level, that these attacks occurred, and also of concern is the fact that a short time later essentially the same method was used by similar attack methodology. So no system is invulnerable, no matter what the investment is. You just cannot take risk away, but you can do the prudent thing, and I think the systems that we have deployed in the United States and the operating procedures that go with them are as good as anywhere in the world, and I think the proof point of that was on July 7, when all of the transit systems in the United States came up on their own to a very high, very effective level of security, and all that work of preparation and vulnerability assessments and all of those things that have been going on for 3 years came up in an instant and was very effective. So I think the security for transit systems in the United States is outstanding.

Chairman COLLINS. Thank you. Senator Lieberman.

Senator LIEBERMAN. Thank you, Madam Chairman. Thanks, Mr. Hawley, for your testimony. Incidentally, Senator Collins raised questions about the allocation of appropriations for mass transit. In fact, in the initial budget proposal by the Administration there actually was a cut from previous levels in mass transit funding, and Senator Collins and I have asked our colleagues on the Homeland Security Appropriations Subcommittee to at least appropriate for mass transit to the level of last year. I hope that you will support us on that. I hope in some sense that this hearing may encourage our colleagues to sustain the current level of funding and hopefully to go higher.

I want to ask you a few questions about the national strategy, and I want to do so mindful of what I said in my opening remarks, that I expect that you will respect the limitations or I will respect the limitations of what you can say and cannot say publicly at this hearing. The strategy has been in the works for a long time, long before you became the Assistant Secretary for Transportation Security, and a lot has happened since it began. There is always a lag time in these kinds of things. I want to ask you this question, which is whether you would say that the National Strategy for Transportation Security, as it was released more than a week ago, reflects the Administration's current thinking on transportation security strategy?

Mr. HAWLEY. Yes, it does. It is a very good baseline on which to build. As you get into it, there is tremendous depth to the information that is there that lays out a very comprehensive look at the total transportation system, and the key point being that in the resource-constrained world, risk-based priorities are the way to go, and that really is at the heart of Secretary Chertoff's strategy for the Department and certainly ours at TSA, and it lays out a lot of the current processes that have been built up of solving the problem of how do we have an effective level of security across systems that operate geographically dispersed and are all interconnected?

How do we connect those with so many different players having responsibility for different pieces?

Senator LIEBERMAN. Let me ask you then to respond in general terms, or however specific you think you can, to my general reaction after having reviewed the strategy, which is that within the itemization in different forms of transportation, of vulnerabilities, there did not seem to be a sense of priorities among those. That is the first one. The second is my own feeling, somewhat explicit, maybe implicit, that the approach to the non-aviation transportation sectors remained much less aggressive, can-do, must-do, even if it is hard, than the strategy for the aviation sector.

Mr. HAWLEY. I can tell you on the transit sector that the first London bombings occurred on a Thursday, and Secretary Chertoff had a number of us in on Saturday with, "OK, what are we doing right now to do what we can to have the level of security effectively increased?"

Senator LIEBERMAN. Long-term, not just——

Mr. HAWLEY. Long-term, I think the strategy gets—it goes back to the point of looking for the terrorists before the attack is launched, and if the predominance of our defenses are only to protect the final end point of the attack, that is not a very good system, and so it is the multiple layers that go to stop an attack before the decision is made by the attackers as to which mode.

Senator LIEBERMAN. That is exactly the point I was trying to make, which is—and I agree with this in part—that if somebody is going to come at a transit system or any other locale in our country, as unfortunately our friends from Great Britain and Israel know, strapped with bombs around their waist, once they get to that point it is hard to stop them, not impossible, as we have seen, but hard. Obviously, the best thing you can do is to have intelligence to stop them before they strike, but I do not want us to allow that reality to be a reason not to do everything we can to protect and defend the final targets, as the British and the Israelis do more than we do, I believe.

Mr. HAWLEY. Yes. I think that is an excellent point, and the things that we can do long-term in terms of technology development and things that tend to be capital costs are not immediately available to us, but a lot of the things—the See Something, Say Something campaign that enlists the public to be alert, training of the employees of the transit operators, behavioral observation techniques.

Senator LIEBERMAN. That's exactly the kind of stuff I am talking about. We are going to hear more about that on the second panel. Can I ask you one final question? After the threat level was raised to orange after the London attacks, local transit systems around the country raised their defense levels, and it put a lot of strain on them in terms of finances. There's an article I have seen from the *Atlanta Journal-Constitution* that reports that raising the threat level to orange this summer cost the Atlanta transit system about $10,000 a day beyond its regular operating budget, which exhausted a quarter of its overtime budget within the first month of the system's fiscal year and pushed the security personnel to work 12-hour shifts even though they had the assistance of local police.

In Connecticut, I can tell you that after the threat level was lowered back to yellow, the Governor announced that State Police officers and National Guard troops would no longer be deployed on the Metro-North trains or at the State bus and train stations. So in some sense the threat level was reduced, as I understood the Secretary's decision, because local protection had gone up, but when the threat level was reduced nationally, the local protection left because of financial reasons. So I wanted to ask you whether the financial strain placed on transit systems by the lack of resources for transit security in any way influenced the Department's decision to lower the threat level for mass transit this past August?

Mr. HAWLEY. The funding source comes from the Urban Area Security Initiative, which has, I think, since September 11, $8.6 billion put into it, and from that pool local communities are able to draw down sources—money from that, particularly to offset overtime, etc.—and I think the issue on when it was time to come down to yellow from orange was based in large part on a sense that we could not keep a high level of alertness at every player across the system indefinitely, and that by the random application——

Senator LIEBERMAN. Because of financial stress?

Mr. HAWLEY. Well, no, just the alert readiness. For instance, it was in the summer, and I saw guys who were in their Kevlar and their helmets, and the approach that seemed persuasive to us is that the random application of parts of orange that would not incur the cost of total orange everywhere, but that random increased patrol here, random dog team there, random different pieces that you did not have to sustain across the entire activity would give a higher delivered level of security than existed at yellow without incurring the cost that you had to have at orange.

Senator LIEBERMAN. I thank you. My time is up. Obviously, I hope you will think about this irony when you lower the threat level, then the locals got rid of the financial stress. I am going to want to ask the Metro police chief, from her perspective, about that whole experience. Thanks very much, Mr. Hawley.

Mr. HAWLEY. Thank you.

Chairman COLLINS. Thank you. Senator Carper.

Senator CARPER. Thanks, Madam Chairman.

Again, Mr. Secretary, welcome. In the airline industry, many technologies have been developed in the military and later made commercially available. Rail and transit systems, however, really do not have the same kind of research and development pipeline to draw from, at least not to my knowledge. How is the Transportation Security Administration working with other agencies in this country or even outside this country to create a similar pipeline for the detection of explosive, radiological, chemical, biological devices that might be deployed against our transit rail systems? How are you working with industry to make such technologies commercially available?

Mr. HAWLEY. On the longer-term improvements in technology, the science and technology group at DHS specifically looks into the science piece to see promising areas. For instance, Senator Levin was talking about standoff detection of suicide bombers. What kind of science could apply to that mission? And so for the longer-term, looking at different, newer technologies and then turning those into

products or providing seed money so that people can create pilots is very much the job of S&T. Within TSA, we have had a very effective explosives lab that is based in Atlantic City, and they spend a lot of time trying to figure out how a particular technology that works in one area could be applied to finding explosives in another. So there is a lot done there, a lot of connection with other parts of the government in other countries. It tends to be a 2-year lag, my guess, before we are going to see that effectively applied.

Senator CARPER. All right. I understand from some discussions we had with folks who run rail and transit operations that they are approached—not besieged, but approached—by vendors frequently who are selling technologies that might help those rail and transit operators to better secure their systems. It is oftentimes difficult for the rail and transit operators to know a good investment from a bad one, as I am sure you can understand. Let me just give you an example: In the area of air quality, EPA has worked with transit agencies and bus manufacturers to set a standard, for example, for low-emission diesel engines that are commercially available. I just wonder how is the Transportation Security Administration doing this kind of thing with security technology? How does TSA determine what technologies are most effective, as well as how those products are most effectively utilized, and how do you get that information to the transit agencies to make sure that they know better how to spend their limited security funds?

Mr. HAWLEY. Senator, I have heard the same comment from lots of people in the transit industry, and the Department, through the State and Local Government Office at the Department—they are the funding source; they are the people that provide the grants—have a kind of Consumer Reports type function that they have where individual technologies are tested and evaluated, and so it is trying to draw the line between saying, "Here is our cookbook, the vendors you should be purchasing equipment from." We do not want to get into making those choices, but we want to say, "Here, these are the technologies that are used in this way and they meet a common standard across the board," so to give the individual transit systems the ability to fine-tune, but also to take the cost of evaluating all those vendors off their backs and let them focus on their own operations.

Senator CARPER. I think you discussed in your testimony the importance of better utilizing canines to detect explosives. To date, TSA has augmented local law-enforcement canine capacity at events like the Democratic National Convention, Republican National Convention, and so forth. Do you have any idea how many canines TSA recommends that transit securities maintain? Is there some rule of thumb that is used in helping them determine that? Do you have any idea how many additional canines are needed for higher-level threat areas and how they have been deployed and prepositioned, and finally what is the cost of providing this level of canine presence and who should bear that cost?

Mr. HAWLEY. The canine opportunity, we have talked about using technology that will join us in a couple of years, but that is a tremendous resource and a very flexible resource, and at TSA we have been on a pretty rapid incline where we expect to finish the year at around 470 dog teams.

Senator CARPER. Any idea what that number might have been a couple years ago?

Mr. HAWLEY. I know last year it was in the 300s, and I don't know really beyond that, but I do know that since the July bombings, we have made 30 dog teams available to 10 large cities, that they will have those dogs by the end of the year. And now, as to the model of how the costs work with dogs, the way TSA does it today is that we have them trained at Lackland Air Force Base, a center of excellence for us for explosives detection, and we pay the operating costs or we reimburse local law enforcement who actually maintain the dog, and then a certain percentage of recipient of that we allocate. For instance, after July 7, we made available a certain number of our airport dog teams for transit operations, and I would say, going further, Senator, speaking specifically of Amtrak, that it is something we are looking at as to how to use any dog team that we have access to, on a random basis, apply it to, for instance, Amtrak or transit systems as requested by them.

Senator CARPER. One last one: You discussed, I think in your testimony, the transit rail inspection pilot program that tested the feasibility of screening passengers, screening their luggage, screening cargo for explosives in transit and rail systems. I think you said this sort of technology might be best used when threats are made against a particular station or site. My question is how will the personnel and technology be deployed when such a threat is identified? Will it be available in every transit system or are you going to have it prepositioned throughout the country and redeployed when a threat is identified, and how also would this be paid for?

Mr. HAWLEY. Yes, the technology works. It is large and expensive and not terribly mobile. Dogs, on the other hand, are available, are mobile, and can be very effectively applied. So my solution is that we keep looking at the technology, keep trying to get the costs down and the flexibility up, but that we have tremendous resources in the canine arena that we are using today and will continue to use as a very effective, mobile, flexible, not terribly expensive force.

Senator CARPER. Madam Chairman, rural southern Delaware has a saying that maybe they have in rural northern Maine about this dog won't hunt, but when it comes to effectively ferreting out explosive threats and that sort of thing on trains and transit, these dogs do hunt, and they do a real good job.

Chairman COLLINS. Thank you. Senator Lautenberg.

OPENING STATEMENT OF SENATOR LAUTENBERG

Senator LAUTENBERG. Thank you, Madam Chairman. I am sorry that I missed an opportunity to make an opening statement, but I would ask that my full statement be included in the record.

Chairman COLLINS. Without objection.

[The prepared statement of Senator Lautenberg follows:]

PREPARED STATEMENT OF SENATOR LAUTENBERG

Mr. Chairman, the natural disaster of Hurricane Katrina was compounded by a disastrous response. There was plenty of warning that a major hurricane could cause widespread flooding in New Orleans. And the warnings came true.

We ignore warnings at our peril . . . but we continue to do so. This month marks 4 years since September 11 . . . and 2 months since the London subway attacks. We know that our transportation system is a potential target of terrorists.

Public surface transportation carries 16 times more passengers than airlines—but we focus almost all our security resources on aviation. In 2002, the FBI warned that Al Qaeda may directly target U.S. trains, rail bridges, and tracks. But despite the warnings, we still don't have a plan to protect our nation's railways.

Since September 11, President Bush has not asked for one dime specifically to secure our rail transit systems. Not one dime. Rather, he asks for a broad Homeland Security fund for the Administration to pick and choose which industries they want to secure and which ones are left to fend for themselves. This is unacceptable. so each year Congress has to designate specific funds for rail transit security needs.

The 9/11 Commission reported in detail how unprepared we were at that time for an attack on our transportation system. Unfortunately, we are still not prepared.

I'm not suggesting airline-style baggage screening, but there are things we can be doing to protect passengers and employees of transit systems that won't inhibit travel. Just like we passed legislation in the aviation sector, this Administration needs specific legislation on rail transit security or it simply won't get the job done.

So while we hold this hearing to discuss "Lessons from London," I hope we understand that the warnings have been present long before July 2005.

Senator LAUTENBERG. As a prelude, very shortly, the natural disaster of Katrina was compounded by subsequent disastrous response, and there was plenty of warning that a major hurricane would cause widespread devastation in New Orleans and the surroundings, and the warnings came true, and we ignore these warnings at our peril, but unfortunately we continue to do so.

This month marks 4 years since September 11, 2 months since the London subway attacks, and we know that our transportation system is a potential target for terrorists. Public surface transportation carries 16 times more passengers than airlines, but we focus almost all of our security resources on aviation. In 2002, the FBI warned that Al Qaeda may directly target U.S. trains, rails, rail bridges, and tracks, and despite those warnings we still do not have a satisfactory plan in place to protect our Nation's railroads. The President, in his budget requests, does not dedicate a particular portion of the funds provided for transit security. Rather, our security is picked out of a group—I say our transit security—out of a broad homeland security fund for the Administration to pick and choose which industries they want to secure and which ones are left to fend for themselves, and I am hoping that this hearing, Madam Chairman, is really timely and very important to bring attention to this exposure that we have.

The funniest thing is when we look at potential attacks or some major incident happening in the rail system, for years we have looked at the transit agencies as having to deal with their own crime on their systems. Terrorist attacks are directed at our society as a whole and our American way of life, and I can think of no greater responsibility for the Federal Government than to protect us in this way. Instead, we have been kind of left to deal with it as part of the total security issue, and it is really not appropriate. I point out that the per-passenger cost for security and aviation is $9.60 per person. The London Underground that we are going to hear more about was over $2 dollars U.S. per passenger. U.S. transit, where we carry 9 billion trips annually, less than a penny per passenger, and it is really imbalanced, as everyone knows, when we saw the terrible tragedy that hit London and Japan in the transit systems, crippling the functioning of that society substantially for a long time, creating terrible problems. So, given your experi-

ence, Mr. Hawley, starting in your position soon after the London bombings, have you seen any sign that the Administration is going to request specific funds in fiscal year 2007 for rail transit?

Mr. HAWLEY. On the issue of specific funds for transit, the Administration believes—and I believe—that the nature of the overlapping jurisdictions and operations in a region such as the National Capital Region or many others, that with so many players involved, that there needs to be some kind of an overview for the area. What is our strategy that is appropriate for this area? And that is why, on the targeted infrastructure protection grants, the Administration proposal for 2006 was up from $300 million to $600 million. So there is a significant amount of money applied to this area, and I suspect that we may disagree on whether it should be targeted directly to a specific mode or made available for them to discuss and distribute as they decide.

Senator LAUTENBERG. Well, a common theme in the development of our intelligence system—the reform of our intelligence system and with the Department of Homeland Security—was focused on the debate as to whether or not the funds should be applied on a risk-based formula. Well, how can we then, Mr. Hawley, in fairness say, "OK, Washington Metro, here is a bunch of money. It is important. Divide it up in ways that you think are most susceptible or most risky"? And to me that does not answer the problem, very frankly, because I assure you there are places in this city that get special funding even though they are perhaps the best protected facilities that we have in the country, but to ignore the damage—I mean, one need only—unless you get a chance to come by helicopter from home—if one gets in the car and drives across one of the bridges and so forth, sees what kind of damage could result from an attack on the Metro. I mean, this place would be in total chaos. So how do we assure that the facility that carries most of the people in the city and its environs is protected sufficiently?

Mr. HAWLEY. Well, clearly the priority for me and TSA and DHS of protecting and being involved in excellent security in the transit sector is very high on all of our radar screens, and the issue of local decisionmaking—one of the 9/11 Commission report recommendations that we take very seriously is the connect-the-dots, and trying to get intelligence from the classified world directly to the operator in a way that they can use it, either by lowering the classification or finding a way to get it unclassified, is an operating way and an imperative that I have of get whatever intelligence that we have, whatever analysis, and network it widely within the industry as best you can from a security point of view, but always relating it to anything that would be tactically of interest and supported completely.

Senator LAUTENBERG. Does the subject of Amtrak ever come up, to your knowledge, under the rail security requirements? I have not seen it mentioned at all in any of the papers that I have seen. Is there anything there?

Mr. HAWLEY. Yes, sir, it is very much a part of it, and as we look at the overall application of our resources and trying to figure what can we use in a flexible way so that we do not focus all our attention on one particular aspect or one particular problem, we do want to have flexibility so we can apply random appearances and ran-

dom security for Amtrak, transit, and all of our responsibilities. So I understand the issue about the funding of aviation versus that of transit, but I can assure you that at TSA and DHS the whole issue of transit security is one that we take very seriously. I spend a great deal of my personal time on it, and we were able to get the deputy transit administrator to come in as deputy at TSA. So we have a very high level, very deep operating experience at TSA, and it is a priority.

Senator LAUTENBERG. I am sure you have seen or heard the expression that came out of a major movie, and that was, "Show me the money," and if we do not see the money we do not know how serious the thinking is.

Thanks very much for your testimony. Thank you, Madam Chairman.

Chairman COLLINS. Thank you, Senator.

Mr. Hawley, before I let you go and we move on to the next panel this morning, I have to tell you that I keep thinking about your response to my last question. You said that, in your judgment, the security of mass transit systems in the United States is "outstanding." I must say I don't know how you could make that judgment when TSA has not finished risk assessments of U.S. systems, and I will ask you to respond either now or for the record.

Senator LIEBERMAN. Madam Chairman, let me just say that I totally agree with you, and everything we know continues to worry me, that our mass transit systems are more vulnerable than they should be today and that we have an urgent responsibility through strategy and through adequate funding to close those vulnerabilities to the best of our ability.

Chairman COLLINS. Thank you.

Mr. HAWLEY. Sure. My basis for saying that was on July 7, the work that had been done over the prior 3 years of actually having written programs and very specific action plans for all of the top transit systems—I saw the top 100—and it was filled out with scorecards of how far they were on a whole variety of individual metrics, and it frankly was a surprise to me to see how ready the American transit system really is, and I make this point not about funding or anything else, but just to say that the work that has been done, consistently done over a 3-year period, has led to a measurable result.

Chairman COLLINS. I think there is a lot of good work going on at the local, State, regional, and Federal level, and by private operators, but I think we have a long way to go, and I will look forward to discussing this further with the next panel. I think until TSA has completed its assessments, it really does not have a complete picture of the state of security for mass transit.

Thank you for your testimony.

Mr. HAWLEY. Thank you.

Chairman COLLINS. I would now like to call forward the witnesses for our second panel. Our first witness, Michael Brown, is the chief operating officer of the London Underground. Mr. Brown has been with the London Underground for 16 years, serving in a variety of operations positions. In his current position, Mr. Brown is responsible for managing the Underground's operations and se-

curity, including emergency planning and response, technology deployment, and personnel.

Our second witness, Polly Hanson, is the chief of the Washington Metro Transit Police. Her experience in law enforcement brings extensive knowledge to this Committee. In the year 2002, after 21 years with the Transit Police, Ms. Hanson was sworn in as the chief.

Our final witness, Rafi Ron, is the president of New Age Technology Solutions, a transportation security consulting firm. Mr. Ron was instrumental in developing and implementing new security policies at Logan Airport. His prior experience includes serving as the director of security at the Tel Aviv Airport in Israel and 30 years in counterterrorism and intelligence services of the Israeli government.

I feel very fortunate that we have such a prestigious international panel giving us a variety of perspectives here this morning. I thank you for being with us.

Mr. Brown, we will start with you.

TESTIMONY OF MICHAEL BROWN,[1] CHIEF OPERATING OFFICER, LONDON UNDERGROUND

Mr. BROWN. Madam Chairman, thank you for your words of welcome, and thank you, Senator Lieberman, and other Members, as well.

It is a great privilege to appear before you this morning. The London Underground is the world's oldest underground railway network. It first opened in 1863. There are 253 miles of routes, 45 percent of the network is in a tunnel system. There are 273 stations on the system served by underground trains, and of these, 255 are operated by London Underground. London Underground provides a public transport railway service to London. It is part of Transport for London, which is a public transport authority under the direct control of the elected mayor of London.

Approximately 3 million passenger journeys are undertaken each day on the Underground network, which is roughly the same number as the whole of the rest of the rail network across the United Kingdom. What I want to do briefly is talk about the security situation before July 7 and then go on to say some of the things that we have done since July 7. We have already heard some commentary about the CCTV systems in the London Underground. At present, the Underground has over 6,000 cameras on nearly all stations and in some of our trains. Within 5 years, that number of cameras will double to 12,000. There are five stations on the network which do not yet have CCTV coverage, but they will have it by June of next year, and that program has been brought forward since the events of July 7.

For all new CCTV systems, every camera will be recorded. Work is also in place to monitor areas that are not effectively monitored at the moment, such as ventilation shafts, more monitoring of car parks and other potential entry points to the network; 6.3 million pounds is being spent on such investment.

[1] The prepared statement of Mr. Brown with an attachment appears in the Appendix on page 58.

At present, policing of the Underground is carried out by over 600 police officers. As of July 8, I ordered an additional 100 police officers, so there will be 750 police officers specifically dedicated to policing the Underground system within a year; 6,000 front-line station staff are deployed across the Tube stations. These staff work either on platform, ticket barriers in local station control rooms, or in control across one or more stations.

All trains have a driver in their cab who is in contact by radio with a line control center. There are seven such rooms across the network. In terms of context, the majority of the attacks before July 7 were carried out by Irish Republican terrorists who had been involved in terrorism in all parts of the U.K., not just in Northern Ireland. They usually, although not always, gave a warning prior to their bombs exploding. So clearly the bombings of July 7 were unprecedented in terms of the type of incident with no warning and being a suicide attack. The Underground is an environment where the millions of people we convey each day have no full check on their identity. No screening of their possessions take place, and there are only ticket gates to control movements in and out of the system.

The phenomenon of the suicide bomber means any traditional measures of detection and interception are therefore likely to be ineffective. Response to the incident is therefore key. After the September 11 attacks in the United States of America, London Underground played a full part in the resilience planning process put in place by the U.K. Government and supported by the Mayor of London. We have seconded a senior manager to the London resilience team since it was established, and this is to ensure that the operational realities of a mass transport metro system can be properly considered in political and investment decisions.

This team has led work in areas such as evacuation of parts of London, chemical, biological and radiological attacks, and most visibly has arranged tabletop and live emergency exercises. The largest of these was a weekend exercise at Bank London Underground Station which simulated a chemical attack at one of the largest, most complex stations on the network. This was a multiagency exercise which was also attended by political leaders. It is my view that the learning from all exercises played a vital role for Underground senior managers in revising training and in their own actions on July 7.

The resilience team also enabled the joint development of a battery-powered track trolley designed to enable emergency service personnel to travel down the tunnel to an incident train while wearing heavy cumbersome protective suits. Although the events of July did not require such protective suits to be worn, these trolleys were deployed to help with casualty and later with body recovery. Also, emergency personnel have been trained to move trains in an emergency with instruction cards being available for emergency personnel to enable this movement of trains. As well as these larger-scale exercises, London Underground arranges every year a smaller-scale live incident gained with the full cooperation and involvement of police, fire, and ambulance services. This usually involves closing down a portion of the network during the weekend where the emergency exercise takes place. While these exercises

cannot obviously involve all members of staff who might benefit from such practical training, in my view they do present a very real scenario for the senior and middle management team to experience and to learn lessons from.

Let me go on to talk about the events of July 7. The three explosions that happened on the Tube network happened almost simultaneously at 08:49 and without warning across the Underground network. Two of the explosions were on trains in the Circle line, both of them in the second car, and one was on the much deeper level Piccadilly line on a train which just departed King's Cross, St. Pancras Station. The tight, deep-level tunnel on the Piccadilly line led to a higher number of deaths and serious injuries here than elsewhere. The fourth explosion on the London bus, as you described, Madam Chairman, took place some hour later and also involved a large number of casualties. It was very close to the Piccadilly line train incident.

In total, 38 people were murdered on the Underground and 52 people in total if you include the bus incident. For upwards of half-an-hour after the incident, London Underground staff were the first responders to the incident before the emergency services arrived. Station staff, train drivers, cleaners, and a large number of managers recovered the dead and the dying in horrific circumstances at all sites. The drivers of all four trains—two were involved at Edgware Road—were among the many that performed with amazing courage, dedication, and compassion for several hours.

As it became clear the scale and nature of the incidents, the entire Underground network system was evacuated. At the time of the explosion, just to put it in context, 500 trains were in service, 2,500 staff were on duty, and the system was evacuated of over 200,000 people in less than 1 hour after the call was made to evacuate (apart from one train that was stuck behind the incident train at Russell Square). This was particularly remarkable as the capacity of the mobile—or as you describe it, cell phone network—was unable to cope with the volume of calls being made by members of the public. So the communication systems in London were at breaking point.

Within 24 hours, 80 percent of the service of London Underground was restored, and this was significant in that it gave a real confidence boost to London and Londoners in the resilience of their city. In accordance with our contingency plan, we put in place a recovery team immediately afterwards, and we restored all services within 4 weeks of the incident, the last part of the network being the Piccadilly line. Five cars remain under police control for forensic examination. Immediately after July 7, all staff were put in high visibility orange vests across the network, all managers with any operational experience were deployed across the network and also asked to wear orange vests. Police deployment was unprecedented with major patrols at the main central London stations, and over the next weeks there would be occasions when every station on the tube network had at least two police officers deployed throughout the operational day in addition to regular station staff.

Enhanced staff briefings were instigated to ensure that train drivers and station staff had rapid access to information as it un-

folded. This proved to be particularly important on July 21 when the three bombs failed to detonate on the Tube, but where the system was kept operational as we were able to describe to staff what the security situation was in real time. Some 17,000 CCTV tapes were removed by the police immediately after the events of July 7, and it obviously was vital that these tapes were replaced. This we did following our normal protocol, but clearly the system was heavily stretched. As you again said, Madam Chairman, the evidence was critical in capturing aspects of the July 21 attempted attacks.

It is also important to note that since the July attacks the criticality of the radio system, the train radio system, has come into question, and what we have done is we have increased the spending on our radio system and have ensured that the delivery of a new system would be brought forward so that all lines would have a new radio system by the end of 2006. In the meantime, we have adjusted operational procedures to ensure that if a radio is inoperative, then we do not run trains in passenger service.

I just want to talk briefly about investment, and I will be talking in pounds, so I apologize for that. Overall investment on the London Underground over the next 5 years will be 5.5 billion pounds. This reflects both London Underground directly managed investment and capital works delivered under our public-private partnership arrangements and public finance initiative contractors. At least 70 million pounds of the public-private partnership works will be spent on safety and security-related improvements over the next 5 years. I have already talked about the CCTV enhancement works and the 6.3 million pounds will be spent on this area. Also, London Underground other works will include improved communication systems by station and train radios and also allow emergency services to use their radio systems underground. The day-to-day operational spent for security and British Transport Police operation has been enhanced following an increase of 100 additional police officers. The annual policing cost directly funded by London Underground is 50 million pounds, and in addition to this London Underground spends an additional 10 million pounds on other security and policing initiatives.

It is worth noting that the estimated revenue impact for 2005–2006 fiscal year of the attacks is of the order of 73 million pounds. As the network returned to normal, it is obvious that there should be a full review of all lessons learned from the event. Obviously, this is not yet in its final draft, Madam Chairman, but what I would wish to share with you is just a couple of things that we have already decided need to be looked at. The first one is car design. There has certainly been some feedback that the location and construct of the internal design of cars may have caused difficulty for some of the immediate rescue and recovery operation. Staff training is undergoing a full structural review within London Underground, and this review has now been extended to include a level of practical rescue and recovery training given to existing drivers and station staff. Already, all staff on the system undergo 5 full days of refresher training every year. The content and duration of this is being reviewed. It is also true that we are reviewing our resource deployment in the event of such incidents and all the issues around multi-site incident management.

Thank you, Madam.

Chairman COLLINS. Thank you. Chief Hanson.

TESTIMONY OF POLLY L. HANSON,[1] CHIEF, METRO TRANSIT POLICE DEPARTMENT, WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY

Ms. HANSON. Good morning, Chairman Collins and Members of the Committee, and thank you for asking me to testify on the Washington Metropolitan Area Transit Authority, or Metro, security initiatives. For the record, I am Polly Hanson, the chief of the Metro Transit Police. My written statement provides general background information on Metro and the Transit Police Department, so I will focus my remarks this morning on our security-related activities.

As the largest transit provider for the National Capital Region, Metro does take its responsibility in homeland security with the seriousness it demands. WMATA's approach to transit security involves a partnership between employees, customers, the transit police, and other public safety departments in the region, as well as the Federal Government. It is a strategic approach that merges the application of technology with enhanced operational awareness and puts an emphasis on training, public outreach, and the use of security assessments that take into consideration the unique features of transit and utilizes many of the industry's best practices to implement these strategies.

My written testimony provides a detailed summary of the security actions taken by WMATA prior to and after the attacks of September 11 in areas such as chemical and intrusion detection, perimeter security, explosives detection, our two federally sponsored security assessments, and other additional target hardening and emergency preparedness measures, so I would like to focus the majority of my statement on the more recent actions Metro has taken in response to the terrorist bombings that occurred in London and in Madrid last year. The actions taken in response to these attacks are designed to enhance both Metro's and the region's emergency preparedness capabilities. Some of the actions taken are the purchase of additional explosive ordnance detection equipment, increasing the frequency of station patrols by transit police special response teams—those are like SWAT teams—who patrol with specially trained explosive-detection canines and semi-automatic long guns. We have purchased additional radiological pages for use on patrol. We have created a multi-jurisdictional partnership with other law enforcement departments in the area to assist with rail and bus sweeps. We have assigned a Metro Transit Police captain to represent the whole transit industry on the FBI's National Joint Terrorism Task Force, which adds to the detective we have had assigned to the FBI Washington Field Office, JTTF, since the late 1990s, and additional security measures that are not visible and are designed that way.

Aside from the actions taken by our transit police, Metro has constantly engaged our customers through a series of public announcements, campaigns, stressing the need to be attentive to their

[1] The prepared statement of Ms. Hanson appears in the Appendix on page 66.

surroundings. During September, National Emergency Preparedness Month, Metro has been sponsoring numerous outreach events for our customers. We hosted an information booth and conducted canine and emergency evacuation demonstrations at the September 1, 2005, DHS kickoff at Union Station. Our safety office has been offering emergency preparedness seminars at the offices of large regional employers, as well as conducting open houses at major rail stations on Tuesdays and Thursdays. During these events, members from the Metro Transit Police, our safety and communications departments, are on hand to answer questions from customers and distribute emergency preparedness brochures to explain emergency evacuation procedures and alternate route planning information that can also be found on our web site, MetroOpensDoors.com. We are also an active participant in the NCR's just-launched emergency preparedness campaign, which has this zip card that allows you to document everything you would need to know in an emergency, and for the first time transportation is a component because of Metro's request that it be a focus because it is so important.

We also think that after Monday night's football game, we might ask Joe Gibbs now to do a campaign because we think people would be willing to listen to him. [Laughter.]

The recent events in London prompted a top-to-bottom reemphasis on our entire workforce on counterterror and emergency response training. Since 2003, Metro bus drivers, train operators, and other operational employees have been shown the National Transit Institute's Warning Signs video, which covers systems security for transit employees, including what to look for and what to do regarding suspicious activity, packages, and substances. Warning Signs is also shown to all non-operational personnel, and we are supplementing our existing training for both operations and non-operations personnel with NTI's terrorist activity recognition and reaction training classes, which focus on suspicious activity and behavior, which I think Mr. Ron will talk in great detail about.

We continue to enhance and expand our training partnerships with the region's first responders with Metro Transit Police-sponsored initiatives such as managing Metro emergencies and the Metro Citizens Corps, both one-of-a-kind programs, and also advanced behavioral assessment training for our regional law-enforcement partners. WMATA's emergency management teams train an estimated 2,000 Federal, State, and local first responders a year at our emergency response training facility. All of this is covered in greater detail in my written testimony.

The Department of Homeland Security and Congress have yet to make the protection of transit infrastructure a top homeland security priority. Less than $250 million of grant funding over 3 years has been allocated nationwide to transit since the creation of DHS in 2003. This amounts to an average of less than 0.3 percent of DHS's annual budget of $30 billion, and prospects are not looking better for the upcoming year.

The catastrophic consequences of Hurricane Katrina, highlighted by the breaching of the levees in New Orleans, serve as a stark reminder of the implications of neglecting to take action to protect critical infrastructure. Given the modest amount of Federal support for transit security to date, DHS could simplify the grant applica-

tion process in fiscal year 2006 to ensure that already identified needs based on both external and internal security assessments are addressed in an expedited manner.

Due to the amount of planning and the approval requirements associated with the fiscal year 2005 transit grant program, most of which replicates what transit systems are already doing, we are now almost a year after the enactment of the fiscal year 2005 DHS appropriations bill and 2 months after the London bombings, and we still have not gotten the green light from DHS to spend our fiscal year 2005 grant funds. At the very least, for fiscal year 2006, DHS should be able to evaluate all the risk assessment information submitted by transit agencies in the past years and provide specific allocations to each transit property based on risk rather than allocating funds on a regional basis. As part of our Metro Matters capital improvement campaign launched in the fall of 2003, WMATA identified $150 million of high priority outstanding security needs, yet WMATA has received only a total of $15 million in DHS transit security grants over a 3-year period. WMATA has allocated most of these funds toward beginning to address the need for redundancy and enhanced reliability for key operations control and communications functions, which was highlighted as a top priority by both our DHS and FTA security assessments.

Other high priority security needs on the capital side include enhancing WMD detection capabilities, expanding intrusion detection and surveillance systems, enhancing decontamination response and recovery capabilities, and additional CCTV capability in rail stations and on buses.

Transit systems around the country work in partnership with the American Public Transportation Association and have played a leadership role in developing security-related best practices in such areas as intelligence sharing, system safety and security guidelines, employee training, emergency preparedness, and the prioritization of transit research projects, but the energy and ingenuity exhibited by the transit sector since the tragedy of September 11 4 years ago must be matched by a greater commitment of resources allocated on a risk basis and practical planning requirements by DHS in order to enhance the security of the more than 32 million customers who ride subways and buses every day. DHS could also do a better job of coordination and information sharing among internal agencies within the Department, such as ODP, TSA, IAIP, and the Science and Technology Directorate.

The transit community also needs DHS's help in the development of standards for detection and surveillance technologies and other security items applicable for target hardening in a transit environment. Metro continues to serve as a test bed for the Federal Government and a model for the country on new security initiatives. Metro's chemical detection system, commonly referred to as PROTECT, has become a model for other transit agencies across the Nation and the world. Working with our Federal partners at DHS and the Departments of Transportation and Energy, WMATA continues to offer training and technical assistance on the PROTECT system to anybody interested in the transit industry. WMATA is actively engaging the Department of Homeland Security in efforts to leverage the advances obtained by the PROTECT

program to other emerging applications in chemical, biological, and explosive detection areas.

In January of this year, the Metro Transit Police and the Department of Homeland Security's Transportation Security Administration collaborated to enhance security at Metro stations and on trains for the Presidential Inauguration. The first-of-a-kind partnership with TSA included the use of Federal screeners equipped with explosive trace detection gear and canine teams supplementing Metro's teams of officers and explosive detection canines. They performed without a hitch and the ops plan developed can be applied to other special events across the country. We were also working with DHS on expanding the application and training of personnel in the area of behavioral assessment screening of passengers in a transit environment.

Early in 2004, WMATA was one of the first transit systems to subject itself to a comprehensive security risk assessment offered by the Office for Domestic Preparedness Technical Assistance Program. It is a useful tool, quantitative and scenario driven in nature and good for evaluating and ranking gaps in our infrastructure protection and response capabilities, and it represents the only example of a DHS agency approaching us with well-thought-out, risk-based process, which allows a property to assess outstanding security needs. And while the assessment methodology needed some tweaking, the ODP assessment team was receptive to our suggestions for improving the process and we recommend that other DHS agencies with responsibilities for accessing transit security such as TSA and the Information Analysis and Infrastructure Protection Directorate work with ODP to enhance and expand the use of this risk assessment tool.

WMATA has a long-standing productive relationship with the Federal Transit Administration on a wide range of emergency preparedness initiatives linked to training and exercises that are also summarized in my written testimony. As the recent events in the Gulf Coast illustrate, considerable coordination and planning among the region's State and local government players, as well as the private sector, is necessary in order to ensure that WMATA's own emergency preparations and security upgrades will provide benefits to the National Capital Region during an emergency.

Using the Metropolitan Washington Council of Governments, or COG, as its primary coordinating body, the region has made progress with regional emergency response planning and coordination. As the lead transit agency in the region, WMATA continues to work with the rest of our partners in the transportation and public safety community to refine the plans in place. My written testimony summarizes other regional emergency preparedness activities that WMATA participates in, as well as our long-standing relationships with the region's other law enforcement departments and emergency management agencies.

We constantly reevaluate our top security needs based on new threat information, updated external and internal security assessments, and emerging technological innovations, and we are going to continue to pursue partnerships with the Department of Homeland Security and anybody else we can find to serve as a test bed for new initiatives in the areas of biological and chemical detection

and enhanced security procedure for a transit environment. The tragic events in the Gulf region reinforce the importance of our need to work with all our regional partners to further enhance emergency preparedness in the National Capitol Region.

Thank you, Chairman Collins, and the rest of the Members of the Committee for the opportunity to present these remarks and for your support of Metro over the years. I am happy to answer any questions you may have.

Chairman COLLINS. Thank you. Mr. Ron.

TESTIMONY OF RAFI RON,[1] PRESIDENT, NEW AGE SECURITY SOLUTIONS

Mr. RON. As a private professional, I would like to especially thank you for inviting me to testify before the Committee.

Over the past 50 years or so, it has become clear that transportation is a high priority target for terrorists and terrorist organizations. Since transportation systems constitute a critical infrastructure without which our modern industrial society cannot function, these systems are very likely to remain at the high-risk end in the foreseeable future. Key links in our transportation systems are vulnerable to attack, and the potential damage may cause a large number of casualties as well as long shutdowns which can lead to major system collapse with multiple economic and political repercussions.

No other system combines such a high level of vulnerability with so many attractive goals for terrorists acting against the United States. As a result of the September 11 attack, aviation security has been given a great deal of attention, and the achievements are impressive. In less than 4 years, the United States of America has set itself as the global leader in aviation security and has become the driving force in making domestic and global aviation systems safer. Unquestionably, American aviation has become a harder target for terrorists to hit. For terrorists, this means that in order to ensure the success of an attack on aviation, they would have to meet much higher requirements than ever before in terms of effort and sophistication. Concurrently, the disruption of global terrorist organizational structure by the U.S. global war on terror is resulting among other things in the shift of responsibility for initiating and executing attacks to local terrorist cells, as we have seen in the cases of Madrid and the London attacks.

The resources needed to mount successful attacks on hard targets are less readily available to terrorists operating on the local level. The important lesson to be drawn from this recent history of terrorist activity is that once high-priority targets are made harder, terrorist efforts tend to be diverted toward minor targets that are still perceived as being soft. Mass transit remains a vulnerable target, more difficult to protect because of its vast extension and accessible nature, because attacking it does not require extraordinary resources, and because technological solutions have only limited relevance to its protection.

The turning of terrorist attention to urban mass transit systems is thus an expected consequence of our success in other domains.

[1] The prepared statement of Mr. Ron appears in the Appendix on page 76.

Implementing the aviation security model in the mass transit environment is not an option; 100-percent screening cannot be performed with the technology available today without creating a bottleneck at checkpoints. However, bottleneck checkpoints are not a proper solution because we need to allow high throughput without which mass transit cannot fulfill its role.

The challenge facing us is to develop a system approach solution that combines technology, human resources, and procedures. This system approach solution must be designed to address the three stages of the security process: preparedness and routine management, incident management and first responding, and recovery. The system must have a so-called open architecture that will allow the shift of weight from one element to the other as more advanced and relevant technology becomes available and operational. At present, the most relevant available technology is in the video field. Traditionally, video systems are installed in the location of the expected crime scene. While this is an effective way to identify criminals and secure the necessary evidence to convict them in court, it is totally inadequate to deal with a terrorist attack because in the latter case, as soon as the attack takes place, terrorist success has been achieved and the damage has been done.

What we need is a new approach to video application, as well as to the overall security planning. Prevention and deterrence must be the goal, rather than detention and conviction. This distinct goal dictates pushing the security measures to the perimeter of the mass transit system. Our focus must be on detection and response before the terrorist gains access to the target. In other words, we need to shift our efforts from the train and the ramp to the station entrances.

While video technology is undoubtedly important, it does not provide us with the most critical information we need, explosive detection. At present, explosive detection systems are designed to meet the requirements of the aviation industry and are not applicable in the mass transit environment. With research and development that will recognize this need and is focused on operational application, such explosive detection systems solutions can be available in the next few years. Current ideas are in the area of air sampling techniques, as well as trace detection on tickets and body parts that come in contact with the system in the entry process.

Appropriate technology is a critical factor for the protection of mass transit systems, but no technology can provide a solution without human individuals who can not only operate it effectively, but also provide appropriate immediate response. It is useless to detect an explosive device if you cannot act to stop the person who carries it from entering the system. Human resources would thus remain a critical element even when we have those future technologies at hand. At the present time, while these technologies are still in the works, the importance of the human factor is even more critical.

In Israel, as well as in other parts of the world, the presence of trained security personnel at entrances to public facilities has proven to be a very effective preventive measure against terrorist attacks, including suicide attacks. Despite numerous attempts by suicide bombers to enter shopping malls in Israel, none has been suc-

cessful. The terrorists were forced to carry out their attack outside the mall. The targets affected have been relatively minor, and the damage sustained was smaller in terms of human life, as well as property.

In reference to the human factor, I would like to point out that the Achilles heel of the suicide terrorist is his behavior. A person intending to commit an extreme act of violence, in most cases for the first time in his or her life, as well as to terminate his own life, is most likely not to behave like the ordinary people around him going about their daily routine. An example is Richard Reid, the shoe bomber, who was clearly detected by both security and non-security personnel as a very suspicious person before and during the boarding process to an American Airlines flight in Paris in December 2001.

Behavior pattern recognition techniques implemented by trained security and non-security personnel have proven to be a valuable measure in the detection and prevention of terrorist attacks in public facilities. The training provides the skills and the confidence not only to law enforcement officers positioned at entry points, but also to employees who are present at every point and corner of the system. No one is in a better position to recognize irregularities on the ground than the people who regularly work there.

Let me sum up by reiterating three major points: One, legacy security programs in mass transit systems must be reassessed in the light of the shift from the threat of conventional crime to the threat of terrorism, including suicidal terrorism. This means putting a higher focus on early detection and prevention. Two, there is a pressing need to invest in technological R&D that will result in effective early detection of explosives and chem/bio material without disruption of throughput. Three, security and non-security personnel in mass transit should undergo counterterrorist training that includes suspicious behavior recognition techniques.

I thank you very much for your attention, and I will be happy to answer any questions.

Chairman COLLINS. Thank you very much. I want to thank all three of you for excellent and very helpful testimony from a real variety of perspectives.

Chief Hanson, I want to begin my questioning with you. You did an excellent job of describing the funding inadequacy, as well as your frustration in the delays in the release of funding, something that Senator Lieberman and I will follow up with DHS on. I want to ask you, given your unusual position of running the Metro for the capital city for a major region with different jurisdictions and handling millions of tourists each year, whether you had any input into the national strategy for transportation security that the Department has recently put together?

Ms. HANSON. WMATA reviewed the document in February and provided comments. I understand the final document is very different and we have not seen it.

Chairman COLLINS. Do you think that you need to have access to this document in order to better understand the roles that different jurisdictions will be playing?

Ms. HANSON. Well, if the document is not shared with the stakeholders, I am not sure I understand what the value is then.

Chairman COLLINS. That is what troubled me as well. The fact that the strategy was initially—until we intervened—issued in a classified form defeats the whole purpose of coming up with a strategy that is supposed to be shared with all the stakeholders so that people understand what their roles and responsibilities are.

Ms. HANSON. I also wanted to say I think right now, for the fiscal year 2005 grant process, there are regional transit strategies. So I am not sure what the relationship is between the national and the regional strategies, and if there is not one, then I do not understand that, either, because it would seem to me that there needs to be a relationship or a connection between those two strategies, otherwise I am not sure why we went through a huge exercise this last grant process in developing a regional strategy.

Chairman COLLINS. I think that is an excellent point, as well, but it troubles me that if the national strategy has not been shared with you, as the person responsible for the security of the subway system in our Nation's capital, then I don't understand who it would be shared with. That strikes me as a real gap or lapse.

Ms. HANSON. And I think most of my colleagues would suggest that we have clearances, so that would not have been an impediment. You did make reference to the fact that it was classified, but at this point most transit properties that have dedicated law enforcement personnel have folks in the agency that have top-secret.

Chairman COLLINS. Mr. Brown, I was very interested in hearing you describe in more detail what appeared to have been a first-rate response to the bombings in London. You have done the training. You had the surveillance cameras. Your response was swift, effective, and undoubtedly saved lives. What is your reaction to Mr. Ron's suggestion that we need to put more resources in at the front end to try to detect and deter someone who is committed to suicide bombing?

Mr. BROWN. Well, I would certainly accept that. I think it is a very valid point. I think part of our approach in terms of the major investment in even more closed-circuit television coverage across the network, as I said, doubling the number of cameras, is just designed to do that. Also, I think there is a need to ensure that all staff—we are compared to many other metro systems—we have a huge number of front-line operational staff visible on our stations. Every one of our stations has staff deployed on them every time that station is open operationally. None of our stations open with no staff on them, and I think we have a responsibility to review how we train those staff to be alert to strange behavior, to people doing different things.

Our staff are pretty sharp. If they work in a station all the time, they know the difference between a lost tourist behaving in a bit of a strange way, looking where to get to Buckingham Palace or something, as opposed to someone who is behaving in a different type of suspicious way, maybe about to perpetrate a terrorist act. So I think absolutely we need to ensure that we do not just rely on police activity or technology, but we also rely on the human factor in terms of our detection capability.

Chairman COLLINS. I think that is an excellent point, as well.

Mr. Ron, what has been the reaction of the public transit agencies that you have approached with your ideas for improving secu-

rity at the front end, aiming at prevention, detection, and deterrence?

Mr. RON. As Chief Hanson mentioned earlier, the Metro system here in Washington, DC, has adopted this approach and is conducting training programs along the lines that we laid down in Boston earlier for the airport environment, and I should compliment the chief for that. We have not seen a lot of that happening in other parts of the country yet, but we do hear about other metro systems around the country that are showing interest in this approach and are looking at the programs to be implemented.

Chairman COLLINS. Thank you. Senator Lieberman.

Senator LIEBERMAN. Thanks again, Madam Chairman.

You have been an excellent panel, very helpful. Thank you.

Chief Hanson, I was really troubled to hear your testimony that you have not gotten the green light to spend the transit money that you did get from the Federal Government for fiscal year 2005. I don't know—Mr. Hawley, you were good enough to stay in the room—do you have a response to that? Just come up to the mike. Do you know what is going on? Is that a typical situation?

Mr. HAWLEY. I do, and I would like to talk to the chief privately about that.

Senator LIEBERMAN. OK. I hope the green light can go on soon because obviously you have significant needs.

I wanted to ask you first a question that, in some sense, the testimony each of you have given has answered, but I want to ask it anyway because I have continued to worry, as we have heard testimony from our own DHS leaders on this, to some extent from Mr. Hawley today, although I think he was more reassuring, that there is a concern that because mass transit systems are more open than aviation, that it is very hard to defend them, so let's not raise expectations too high, because I think that ends up creating a pessimism that also encourages less defense than we should have. And I understand the difference, obviously, between getting on a metro and a train, and getting on a plane, but I presume you agree that there are a lot of things nonetheless that we can do. I mean, it is great to say that better intelligence will stop a suicide bomber before he or she gets to the Metro or the Underground or the bus station, but some of them are going to get through and then we have to figure out how to stop them as they get closer. So am I correct in what I have heard? Do you agree that we have to approach this with a can-do, must-do attitude about mass transit security?

Mr. BROWN. Absolutely, Senator. My view is—and I just go back to the comment I made—that if you think about the lost revenue that we have had as a network of 73 million pounds for this fiscal year—that in itself actually should be part of the investment decisionmaking process. This makes commercial sense, never mind all the human factor sense that it makes. I think things like the portable detection device, limited use of some screening of people coming into stations, is certainly something we are exploring on a targeted basis.

Senator LIEBERMAN. There would be a random screening or a screening after some kind of behavioral identification?

Mr. BROWN. Well, it could be either, and also it could be based on specific intelligence, because there's no doubt there is intel-

ligence in the background in all of this, and therefore it is minimizing your risk on these things. I think also, to the point that was made earlier on in terms of the amount of approaches that you get from all sorts of people who are selling you bits of kit that are going to solve all your problems, I have to say I think 99 percent of those that I get go straight in the trash can because really most of them are not worth the paper they are written on. So I think we have to, as an industry, work very hard to ensure that we have confidence, globally have confidence, to ensure that we are deploying the right technology, that we are using the right expertise, to ensure that we do target our resources effectively, but certainly not targeting any resources cannot be the right answer.

Senator LIEBERMAN. Right. Chief Hanson, I was impressed by your description of some of the things the Metro system here is doing, and obviously—are you working at all with random searches? I know in Connecticut on the trains, when the orange alert went in after the London bombing, that there was some random searching of people done. Have you experimented with that?

Ms. HANSON. We are analyzing that. We are putting together a package that I am actually going to present to both the CEO and the Board of Directors for Metro to discuss ideas that we have. I support Mr. Ron's ideas—and WMATA has taken advantage of the training that is based on his philosophy and teachings. I have been very fortunate in this region to be able to access Urban Area Security Initiative money. I am the exception, not the rule. Many of my counterparts in the country do not have as much success accessing the regional money as I have. We have paid for some of that training with that money, and I have received money for the orange alert overtime. But as Mr. Brown mentioned, he has 8,000 operational employees. We have the same. It is very expensive to train operational employees, and I am not talking about the cops. There is reimbursement money for them. With your operational employees, you cannot take a bus driver off the bus and not replace him or her. If some of the training that is available through use of Urban Area Security Initiative money was there to support the training of operational employees, then that would be a more effective way of promoting prevention activities because then you are drilling down and using all your employees to be effective in the prevention or identification of suspicious activity.

Senator LIEBERMAN. Well said.

Mr. Ron, am I right that—I believe you talked about this, or at least in your written testimony—that in Israel the operational personnel, bus drivers, for instance, are trained in some of these detection techniques?

Mr. RON. Yes, they are, and that actually comes into effect by more than one—the suicidal attack that was completely and successfully prevented on the field by bus drivers that identified the terrorist as he was boarding the bus——

Senator LIEBERMAN. Right.

Mr. RON [continuing]. And responded immediately and correctly by either closing the door on the terrorist and not allowing him to board the bus or by even pushing him out of the bus if he was already on the bus, and we have more than a few cases where these tend to save a lot of lives and was very successful.

Senator LIEBERMAN. I was struck by one thing you said, very sensible, it seems to me, that it's a different way to go at the disproportionate allocation of funding to aviation security here, which we all support, but one of the effects of that is that it makes mass transit more of a target because it is softer, it is more vulnerable. On my time, which is running out, I want to ask you just to talk a little bit more about—you mentioned how security personnel are stationed now at the entrance points to major bus stations to deter terrorists from coming there so if they're going to strike they will go to a bus stop where there are fewer people, same with the malls. I was fascinated by that. I assume you mean that they are trained in this behavioral pattern recognition that you have talked about. Just take a moment to tell us what does that involve and, in a very American context where there is always a debate about profiling, does it include profiling as part of that?

Mr. RON. Well, I will start from the last point since I recognize the sensitivity of the issue of profiling, and I would like to emphasize that the program that we are advocating is not a racial profiling program, and I would like to make that very clear. This is behavioral conduct that has nothing to do with any racial or ethnic aspects, and I would even like to emphasize the point that our experience in Israel has taught us, especially at Ben Gurion Airport in Tel Aviv, that terrorists do not come in the shape and color that everybody expects them to be. The two worst attacks on Tel Aviv Ben Gurion Airport, one was carried out by a group of Japanese terrorists and the other one was carried out by a German terrorist. Another attempt to take a bomb to an El-Al flight from London was carried out unknowingly by an Irish young pregnant girl. So this is very much as far as one can get from the racial profile of what we all expect to be a terrorist, and I strongly suggest to avoid racial profiling, also on professional background, not only on moral and legal background.

Now, as far as the training that takes place in Israel to employees and the issue of positioning them at entrances to public facilities, training defers from one agency or one entity that carries out the security work to another, but the common denominator is the idea to detect a potential terrorist or to detect suspicious individuals before they manage to enter the premises or the facility that is being protected. In Israel, by law, every public facility, including coffee shops and restaurants, must have a guard at the door, not to mention the major bus stations and train stations, and this is carried out by the facilities. It is paid by the businesses. They protect themselves, and they are using private security companies. The level of training of the private security companies is not regulated in Israel, but there is common knowledge that is shared among the people in the industry, and this has proven to be very useful.

As far as the government agencies that are in charge of protecting public facilities, including the railway system or the railway main terminals, the airport main terminals and etc., these are being trained in the same philosophy that I mentioned earlier, and this has proven to be very successful.

Senator LIEBERMAN. Well, thank all of you, the three of you, for what you are doing and for what you have helped to teach us about

what more we can do here in the United States to protect riders on mass transit.

Chairman COLLINS. Thank you. Senator Lautenberg.

Senator LAUTENBERG. Thank you again, Madam Chairman, for conducting this hearing and for being able to identify the excellent witnesses that we have had here today, different perspectives, but all focused on the same problem. I would have to say that the traditional perspective that the police chief is this tough, burly guy who has large muscles certainly does not seem to apply, and I feel very comfortable, however, and very safe with this very excellent presentation by this relatively, almost—I will not say harmless looking—but not menacing at all, and it is nice to see that.

Ms. HANSON. You are too kind.

Senator LAUTENBERG. It is nice to see you and to hear what you have to say about the system, and you raise some very serious questions for me. And you say, at least in your testimony, for fiscal year 2006, DHS should be able to evaluate all the risk assessment information submitted by transit agencies in the past year and provide specific allocation to each transit system based primarily on risk rather than allocating funds on a regional basis. And Senator Lieberman took the liberty of referring a question to Mr. Hawley, because as I heard your remarks, Mr. Hawley, I thought that you were kind of accepting the fact that these funds have to be given out regionally and it is left to others to decide precisely how the distribution is going to be made.

Now, in each case here, you have a different perspective on the transit systems. Israel, for instance, does not have, or maybe they have had and you never know quite what is on the agenda in Israel at any given time, but very little rail system use for commutation. I think that helps, doesn't it, have a better control factor about who is coming and who is going? We have heard a lot about the heroic actions by bus drivers, by people who traditionally have a very limited responsibility, but reacting to danger and the reaction saving lots of lives and encouraging people that they can still use the system and believe that they are being protected. We had a woman from New Jersey killed some years ago on a bus, and I happened to have been traveling in Israel at the same time, and it was amazing—and I will venture to a side perspective. I was sitting, with several Senators, with Prime Minister Sharon, and all of a sudden, in the middle of the meeting—Senator Rockefeller was there, Senator Levin, Senator Reid—we were on our way to Iraq and notes were being passed to the Prime Minister, and he looked crestfallen all of a sudden. And he said, "We have just learned that there was an attack at Ashdod by a couple of suicide bombers, and they took a number of lives." And I volunteered, and I said, "Mr. Prime Minister, you don't have to continue this meeting. This is not urgent. This is informational, and we understand you have got other things to take care of." And he said to me, "Senator, a Prime Minister in Israel knows only one thing, that whatever happens, he must carry on, and we are going to carry on this meeting." I was struck by that, by that commitment. We all have the same commitment, expressed differently.

Mr. Brown, the reaction of your people in London—I do not know whether you had seen the film—it was called "A Dirty Bomb"—that

was run some weeks before that, using London as an example, and I do not know whether that induced that violent behavior or what, but your performance was far better than that movie indicated. So I did not mean to use my time making a speech, but I wanted to ask how much help, for instance, does WMATA get from city police, from Capitol Police, in terms of your security?

Mr. Brown, how much help do you get from London City Police or national police? Is that a significant part of your security network?

Mr. BROWN. If Chief Hanson allows me to go first, yes, certainly in London the British Transport Police is responsible for policing the public transport network, but in times like July 7, the boundaries kind of disappear. So the Metropolitan Police actually were the ones that led the investigation. The Metropolitan Police across the whole of the United Kingdom has a particular role in antiterrorist activity and terrorism investigation, and therefore they took——

Senator LAUTENBERG. That was after—and I think, Mr. Ron, you made a point about having the intelligence.

Mr. RON. Yes.

Senator LAUTENBERG. The capacity to interrupt was something else.

Mr. RON. Yes, absolutely. So there was a huge engagement of lots of policing, and, in fact, we had police officers down from Scotland and from all parts of the U.K. in London immediately after the events. So it was a national response to an attack on our nation's capital.

Ms. HANSON. Sir, we have also regional partners, and I would have to say you mentioned your own Chief Gainer, as well as Chief Ramsey, and part of the partnership initiative I discussed is something that we created right after the London bombings that we are sustaining—and it is police officers from jurisdictions throughout this area—Fairfax County's helicopter, as well as bicycle cops from Montgomery County, or transit cops with Capitol Police officers, as well as MPD, do sweeps together of stations and buses. In fact, we also brought in commanders from the regional police departments to this initiative, and brought in our regional partners from VRE, MARC, and Amtrak to explain where our vulnerabilities and risks were so that folks in the region knew and created a document for regular police officers so they would be attentive to our critical infrastructure. And Mr. Ron's training that he created, we actually shared with our regional partners that are a part of this sweep team, because we do want to share with anybody we can the vulnerabilities, the special features of transit, and the things that, if you are not a transit cop or a transit employee, you might not be attentive to.

Our Managing Metro Emergencies was created to bring our regional law enforcement partners, fire department first responders, as well as other emergency managers together in a classroom setting to go over transit-specific incidents so that it would allow first responders who have to come to an incident to be well-versed and trained in the intricacies of transit so that we have a better, stronger first response in this region. So partnerships are not a problem for us, sir.

Senator LAUTENBERG. I will conclude with—because I am frankly stuck on the fact that we all talk about how dangerous, how devastating an attack on a transit system could be, and we should be working so hard to prevent it. Again, I think, well, London, Madrid, Japan—I mean, we have seen it in all those places—creates—as you said, Mr. Brown, it is the economic consequences, though it is secondary to the human consequence—the fact of the matter is that it affects people's lives in adverse ways all over the area or the country. So when I look at Chief Hanson and your commentary, you say WMATA identified—as part of the Metro Matters capital improvement campaign launched in the fall of 2003, WMATA identified $150 million of high priority outstanding security needs, yet WMATA received only a total of $15 million in DHS grants and securities. Now, are you still lacking the kind of support that you think ought to be coming? And we recognize there is all kinds of competition, but what do you have to have to protect the people that use your system? It is a very efficient system. It is a very pleasant system to ride, and it has attracted a huge ridership as a consequence of that, and security seems to be a given there.

Ms. HANSON. On the issue of the people we are transporting—it's worth noting that Metro was essentially created to support the Federal Government, and almost 50 percent of our riders come here to the core of the city and are Federal Government employees. We only have to look at the example of Hurricane Isabel. Metro, because of information we received, chose to shut down because we thought the winds sustained would be too much to run the rail and bus system safely. And when we shut down, this region shut down because folks had no other way to get to work. The effect on the economy and commerce in this region would be tremendous if Metro could not run.

There is some operational flexibility that the London Underground has, as well as New York, because they are older systems, that WMATA does not have. We have a two-lane highway, one going one way, one going the other. We do not have another lane, and you know what happens on I–95 or even out here on Independence Avenue if you have something stuck in the roadway. So we are very vulnerable if we had something happen to our system. While we would run to the extent that we could, our ability would be really limited, and many of the things that are in our improvement plan, Metro Matters, have to do with capacity, have to do with our need to be able to carry not just the passengers we are challenged to carry now, but additional folks we might have to evacuate, and to improve our communication train control systems, which I think you had Mr. Brown saying were very important. So it is very important. We do need the support. We continue to use the funds that we get to go down the list of priorities as established by our risk assessment done by ODP, which is part of DHS.

Senator LAUTENBERG. Senator Collins and Senator Lieberman, we have had lots of discussions around these areas of how grants should be made, and when we hear it from such an authoritative, experienced voice and we see the result of a good performance—and we admire what you have done, Mr. Brown, and you, Mr. Ron, and I am glad that Mr. Hawley was locked into his chair and could

not leave the room—is Mr. Hawley here—because we are going to be back again and again and again.

Thank you very much.

Chairman COLLINS. Thank you.

Mr. Hawley, I do want to commend you for staying to listen to this panel. I know that you, as well as the Members of this Committee, have learned a great deal from their testimony, and we will look forward to having additional conversations with you.

I very much appreciate the participation of all of our witnesses today. This is an extraordinarily important issue, and it should not take yet another attack on a mass transit system, whether here in the United States or somewhere else in the world, for us to focus on improving mass transit security. My hope is that this hearing, which was recommended by Senator Lieberman, will help to focus the attention of policy makers and make this a priority, as all of you have urged.

I want to yield to Senator Lieberman for any closing remarks, but I very much appreciate your testimony.

Senator LIEBERMAN. Thanks, Madam Chairman, a personal thank you for your focus on this problem. Even in the midst of all our work in responding to Hurricane Katrina, we cannot take our eye off of this because the terrorists are not—and I think this has been a very constructive hearing.

Just to pick up from what you said a moment ago, there is always a danger—and I know when you are in an open society, as we are, and the two other countries represented here are, there are a lot of soft targets. You cannot protect everything, but there is a way in which we have got to, as I think we are all trying to do, get ahead of the terrorists. In other words, we cannot be always responding to the last attack and fortifying that previous target. We have to get on thinking—the 9/11 Commission, in its extraordinarily impressive report, said that, memorably, one of the great deficiencies here in the United States in terms of preventing such an attack was a failure of imagination, and what did they mean? They meant our inability to imagine that people would actually do what was done to us on September 11, and now, shame on us if we are not actively trying to put ourselves into the brains of these evil forces that hate us, to think what is next so that we can get ahead of them to stop it.

I think the three of you have contributed both to the defense of the people you have the responsibility to protect, but have also helped us greatly. And I also thank Mr. Hawley for staying here, and I hope that it has been as valuable for him to hear your testimony as it has been for our Committee.

Thank you very much.

Chairman COLLINS. Thank you. The hearing record will remain open for 15 days for the submission of additional materials. I want to thank our staff for their hard work, as well, and this hearing is now adjourned.

[Whereupon, at 12.15 p.m., the Committee was adjourned.]

APPENDIX

UNITED STATES DEPARTMENT OF HOMELAND SECURITY
TRANSPORTATION SECURITY ADMINISTRATION

STATEMENT OF KIP HAWLEY
ASSISTANT SECRETARY

Before the

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

September 21, 2005

Good morning Madam Chairman, Ranking Member Lieberman, and Members of the Committee. I am pleased to have this opportunity to testify on the subject of protecting public transportation targets from terrorist attack. My focus today will be on the programs and initiatives of the Transportation Security Administration (TSA) in mass transit and rail 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 9/11 attacks. We are charged with protecting all modes of transportation – a mandate we have taken seriously since our inception. 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 tactics of our enemies and of the need to remain vigilant and prepared.

The Department of Homeland Security (DHS), jointly with the Department of Transportation (DOT), delivered to Congress on September 9 a National Strategy for Transportation Security (NSTS), called for by the 9-11 Commission, the Intelligence Reform and Terrorism Prevention Act of 2004, and the Conference Report accompanying the Homeland Security Appropriations Act, 2005.

While the report itself is classified, and therefore its details cannot be discussed in a public forum, the NSTS outlines the Federal Government's approach, in partnership with state, local, and tribal governments and private industry, to secure the U.S. transportation system from terrorist threats and attacks, and prepare the Nation by increasing our capacity to respond if either occurs. It describes the policies the Federal Government will apply to manage the transportation risks and discusses how the Government will organize its resources to secure the transportation system from terrorist attacks.

The NSTS applies a threat-based, risk-managed approach, using the factors of threat, vulnerability, and consequence, to evaluate asset categories in the six transportation modes: aviation; freight rail; highway; maritime; pipeline; transit, commuter and long-distance passenger rail. This evaluation identified asset categories at greatest risk for each mode, for which corresponding risk-based priorities were developed. The document also discusses the roles and missions of Federal, State, regional, local, and tribal

authorities and the private sector, response and recovery responsibilities, and research and development requirements.

Our Current Program

Efforts to ensure transportation security vary with the nature of the system involved. The Nation's passenger 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 – intercity rail, commuter rail, subway, 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, the security mission for those systems needs to be different. Many passenger rail and mass transit systems are vast in terms of infrastructure and ridership. To provide 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.

Because passenger rail and mass transit systems are networks interconnecting multiple carriers, routes, access points, and transfer hubs with massive passenger volume and flow, broad geographic spread, and multiple branches and interconnections, we cannot simply graft our commercial passenger aviation security systems now based on fixed and controlled checkpoints onto the passenger rail and mass transit modes. That is not practical. Instead, we have, since our inception, been working with those operating the rail and transit sectors to get in place an overlapping, flexible, multi-layered security regime. There is a strong security base in place and with continued close communication and a sense of urgency, it will continue to improve. I would like to address three areas of focus going forward: stakeholder partnership and cooperation, risk assessment, and technology evaluation.

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 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 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 for rail and mass transit activities.

On September 6, I signed an Annex to the existing DHS/DOT Memorandum of Understanding (MOU) on public transportation security with DOT's Federal Transit Administration (FTA) and DHS's Office of State and Local Government Coordination

and Preparedness (SLGCP). This MOU Annex cements our already solid, effective working relationship with FTA and SLGCP and delineates lines of authority and responsibility. This partnership will move us forward as we draw upon each organization's strengths to better provide services and information to the Nation's transit community. We designed this Annex with the goal of ensuring that programs, means of delivery, and protocols for incorporating stakeholder feedback are fully coordinated.

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 mass transit and rail systems to balance risk with resources. TSA's initiatives are intended to focus the collective limited resources available on the prevention of terrorist incidents with the greatest potential consequences.

Technology Evaluation. The challenge of harnessing security technology for mass transit and rail is two-fold: How can we best adapt the security technology developed for other purposes to the very different environment and circumstances of mass transit and rail systems? What new technologies are uniquely suited to mass transit and rail systems? Pilot programs, exercises, and research and development aim to leverage current and emerging technologies to deter attacks against mass transit and rail 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 assisted the 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 authorities 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 $8.6 billion for general counterterrorism preparedness. The President's Fiscal Year (FY) 2006 homeland security budget proposes an additional $2.4 billion for this purpose. These funds can also be allocated by State and local governments for rail and mass transit security efforts. The FY 2006 budget also requests $600 million – a more than 60 percent increase – for the Targeted Infrastructure Protection Program, which covers security for rail, mass transit,

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.

TSA has also coordinated closely with 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 by 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 continually identify best practices to enhance security in the mass transit and rail modes. We are committed to maintaining these engagements and using the information and experience gained in security measures and programs. TSA conducts weekly stakeholder teleconferences where unclassified threat information can be discussed, and TSA has a Surface Transportation Information Sharing and Analysis Center (ST-ISAC) at the Transportation Security Operations Center to prepare and distribute threat information to the mass transit and rail transportation industry.

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 transportation 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, to establish a baseline on the state of security in the Nation, and to establish performance-based security standards. This data also assists TSA in identifying areas where additional resources need to be dedicated to address security shortfalls.

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. A total of 95 inspectors have been hired, and all 100 inspectors will be on board in the next 60 days. The inspectors will identify gaps in security and inspect for compliance with the SDs.

Transit and Rail Inspection Pilot Program. 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 provided $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 to

assist in security efforts on transit systems, ports, and other transportation related activities, 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 2005 Presidential Inauguration and the 2004 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 rail and local mass transit 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. For example, TSA partnered with the Metropolitan Atlanta Rapid Transit Authority, deploying six TSA-certified explosives detection canine teams throughout that system.

Explosives detection canine teams bring technical capability, mobility, and flexibility to security – attributes essential in protecting network systems. The canine teams can move throughout the system, and they can also post at multiple points during time periods that vary by shift and by day. This variability in locations and times for use of canine teams adds an important element of unpredictability to enhance security.

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. Participating law enforcement officers 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 9/11. DHS and DOT have been working 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's 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. Based on the study, the Secretary of Homeland Security recommended that the Department of Transportation maintain the current placarding system.

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 to address compliance issues involving tank car design, construction, quality, and maintenance.

Freight Rail Security Demonstration Projects. TSA has partnered with SLGCP to develop projects as part of that Office's FY 2005 Freight Rail Security Program (FRSP). These demonstration projects will be funded this fall with $5 million allotted from the appropriation in the FY 2005 DHS Appropriations Act to SLGCP 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, SLGCP, 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. This tool is available on TSA's website. 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. 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 rail lines, tunnels, bridges, mass transit systems, and bus terminals/systems 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 our transit systems generally, as well as the way in which we interact. 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'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. TSA personnel were given access to transit agencies' operations centers nationwide to observe and evaluate and assist in responsive measures. 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.

We also gained valuable experience in crisis communication among all parties, internal and external to TSA and DHS. Secretary Chertoff's decision to elevate the risk level to "Orange" for only this sector gave us valuable data relating to the ability of non-transit entities that were at "Yellow" to offer assistance to their "Orange" counterparts.

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, Israel, Spain, Russia, 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 TSA 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.

On a multilateral basis, TSA has addressed the issue of rail and mass transit security in several existing forums, such as the European Union-United States Transport Security Cooperation Group and the Asia-Pacific Economic Cooperation (APEC) Transportation Security Working Group. TSA is also addressing rail and mass transit within the Group of 8 (G8) Secure and Facilitated Travel Initiative. TSA is cooperating closely with Japan in its efforts to host a 2006 Japan Transport Ministerial Meeting, which will include on its agenda rail and mass transit security.

The Road Ahead

We go forward with a disciplined measured program for protecting our mass transit and rail systems. Our efforts will continue to emphasize the shared responsibility of the Federal government, State and local governments, and industry. 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 ensure 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 mass transit and rail 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 ensure 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 mass transit and rail security. I will be pleased to answer any questions you may have.

Questions for the Record
Senate Homeland Security & Governmental Affairs Committee
"After the London Attacks: What Lessons Have Been Learned to Secure U.S. Transit Systems?"
September 21, 2005
Assistant Secretary Kip Hawley

Questions from Senator Susan Collins

1. Congress, GAO, the 9/11 Commission, and others, have recommended a risk management approach to securing the transportation system. DHS leadership has also recognized the importance of adopting a risk management approach, and TSA has repeatedly reported that it has adopted this approach in securing transportation systems. Yet, TSA has not completed risk assessments of the nation's passenger rail systems.

A. Why have these assessments not been completed to date, and when can we expect them to be completed?

Response: Risk management in the transportation sector is a shared mission across the Federal government. TSA is a primary stakeholder and conducts assessments of its own, but it also leverages risk assessments being performed by various federal agencies. Extensive assessments have been conducted in the passenger rail and mass transit mode, and we are building upon this work. For example:

- DHS/TSA has leveraged the security assessments done by the Federal Transit Administration (FTA) and Federal Railroad Administration (FRA) following 9/11, and has developed a gap analysis based on that information;

- DHS/TSA, with DOT's technical and operational support, has completed 27 Corporate Security Reviews (CSRs) on key rail and mass transit systems. In addition, through technical support associated with the Transit Security Grant Program, the DHS Office of Grants and Training (G&T) has completed or has in progress facilitated system risk assessments at 25 of the Nation's largest transit properties;

- DHS/TSA has completed over 2,600 criticality assessments for particular components of rail/mass transit systems, including 848 in rail and 1,778 in mass transit; and,

- DHS/TSA has developed the Vulnerability Identification Self-Assessment Tool (VISAT), a multi-modal tool that public transportation agencies can use to self-assess vulnerabilities of their systems.

TSA is also leading a Risk Management Task Force with representation from DHS's Office of Infrastructure Protection, Customs and Border Protection, U.S. Coast Guard, and Office of Grants and Training, as well as the Department of Transportation and the Department of Defense. The task force will better define the roles, responsibilities, and processes for risk assessments across the entire transportation sector to improve information sharing and reduce redundancy. The findings of this task force will be documented in the Transportation Sector Specific Plan of the National Infrastructure Protection Plan.

Questions for the Record
Senate Homeland Security & Governmental Affairs Committee
"After the London Attacks: What Lessons Have Been Learned to Secure U.S. Transit Systems?"
September 21, 2005
Assistant Secretary Kip Hawley

B. If TSA has not completed the assessments, how can we have confidence that the agency's security efforts are appropriately targeted?

Response: The Transportation Security Administration (TSA) and the Congress have focused the majority of transportation security resources towards what has been considered the highest risk threat: attacks on our aviation system. At the same time, TSA utilizes the broad range of intelligence it receives, as well as the domain awareness gained through the risk-based assessments described above, to inform the development of strategies and programs to improve security in other modes of transportation. One important initiative that has emerged from this approach is the development of Multi-Modal Security Enhancement Teams, which during increased threat levels are deployed by TSA to assist transit, railroad, and local police agencies to enhance security visibility in a variety of surface transportation modes. The teams consist of a mix of Federal Air Marshals, Aviation Security Inspectors, National Explosives Detection Canine Team units, and Surface Transportation Security Inspectors. The teams will also be routinely deployed to ensure that they are familiar with the transit environment and safety procedures.

2. Pursuant to appropriations last year, TSA hired 100 rail inspectors. Can you tell us how you will be using these inspectors and whether industry had any role in developing the compliance and inspection program?

Response: The Transportation Security Administration (TSA) has now trained and deployed these 100 Surface Transportation Security Inspectors (STSIs) to passenger rail and mass transit systems. To date, the STSI program has focused on nationwide outreach and liaison activities with the rail industry, and initiatives aimed at enhancing security in passenger rail and mass transit systems. STSIs are actively engaged in performing Security Analysis and Action Programs, which systematically examine a stakeholder's operations to assess compliance with security requirements; identify security gaps; develop best practices for sharing across the mode; and gather baseline information on the system, its operations, and its security resources and initiatives. In addition, STSIs conduct System Security Evaluations to comprehensively assess a system's security posture, as well as Security Directive Reviews, which are more focused assessments of compliance with the applicable Transportation Security Administration Security Directives.

In addition to their security assessment responsibilities, STSIs have been deployed to enhance security and domain awareness during significant events. On July 7 and July 21, 2005, STSIs deployed jointly with DOT's Federal Railroad Administration Safety Inspectors to monitor security postures and provide the Transportation Security Operations Center (TSOC) with security situational awareness in response to the London bombings. STSIs also deployed to support recovery efforts in the aftermath of Hurricanes Katrina and Rita and to provide enhanced security for the Presidential Inauguration and the Super Bowl. STSIs also regularly deploy to support investigation of transportation security incidents.

Questions for the Record
Senate Homeland Security & Governmental Affairs Committee
"After the London Attacks: What Lessons Have Been Learned to Secure U.S. Transit Systems?"
September 21, 2005
Assistant Secretary Kip Hawley

As part of an ongoing TSA effort to develop surge capacity to enhance security in mass transit and rail systems, STSIs provide security presence and subject matter expertise on Multi-Modal Security Enhancement Teams. These teams generally consist of Federal Air Marshals, Aviation Security Inspectors, National Explosives Detection Canine Team units, and STSIs, and serve to supplement local security resources and gain enhanced domain awareness and security capabilities.

3. The use of closed circuit television, deployed widely in the London Underground, enabled a swift, successful law enforcement investigation following the July attacks. Should U.S. systems more widely deploy this capability?

Response: The City of London (as well as the London Underground) utilizes a network of closed circuit television cameras to assist with criminal investigations, traffic control, and other matters. This network played an important role in the post-incident analysis phase of the London attacks.

While closed circuit camera systems can be useful, each U.S. transit system has particular structural and operating characteristics that affect the application of technology in its security program. As a result, the best security system to meet the needs of different transit systems varies widely.

Funding from grant programs administered by the Department of Homeland Security Office of Grants and Training and DOT's Federal Transit Administration may be used to offset costs associated with installation and maintenance of camera and communications systems for security. The Department of Homeland Security (DHS) has also established research and development priorities to develop and test technologies to support mass transit in the area of threat detection and surveillance. DHS is working with transit operators to establish performance standards for such technologies, and to solicit proposals from vendors for product solutions to meet those standards.

Questions from Senator Carl Levin

Explosives Detection Technology

- **Current Research and Development Efforts**

1. I understand that the technology for the detection of chemical and biological agents is more developed than the technology for the detection of explosives from a distance, and that chemical and biological detection technology is already strategically deployed at critical transit systems and urban areas across the country.

A. About how much money is being invested in research and development of explosives detection technology, and where are the investments being made? Please provide a breakdown

of the data showing federally funded research versus privately funded research.

Response: In the Science and Technology (S&T) Directorate, efforts will continue to focus on developing the ability to detect, interdict and mitigate the consequences from aviation threats and improvised explosive devices (IEDs), both suicide bombs and vehicle bombs, approaching high profile targets and densely populated areas.

Aviation Security: The S&T Directorate will complete the air cargo pilot to evaluate available technologies to screen break-bulk air cargo. The prototype automated carry-on baggage explosives detection system will be evaluated and readied for qualification. Current passenger explosives detection systems will be improved and evaluated. The development of advanced systems to screen people for both explosives and weapons will continue to be pursued. Also, as improved systems become available, checked baggage explosive detection systems (EDS), checkpoint screening, and cargo screening systems will be evaluated for certification or qualification. Current FY 2006 funding is $109.7 million with approximately 43 percent directed toward federally utilized research and development (R&D), e.g., Federally Funded Research and Development Centers and Department of Energy National Laboratories, and approximately 57 percent utilized in privately funded research.

IED Detection: The S&T Directorate will pilot commercially available and prototype suicide bomber explosives detection systems in operational environments; approaches include automated X-ray systems, trace detection systems, millimeter wave and canine teams. Prototypes of advanced systems to screen people for suicide bombs will be developed. Also, a pilot to test commercially available and prototype systems suited for vehicle screening will be conducted. The S&T Directorate will continue the development of stand-off vehicle bomb detection technologies, e.g., laser induced breakdown spectroscopy. Explosives detection research is being pursued in the areas of nanotechnology, biosensors, advanced physics, and advanced signatures and systems. Current FY 2006 funding is $16.4 million. Approximately 50 percent is directed toward federally utilized R&D and approximately 50 percent will fund the private sector to develop explosives detections systems for suicide and vehicle bombs (e.g., millimeter-wave, Terahertz, and quadrupole resonance).

B. Who are the key companies, academic institutions, or others conducting this research and development into explosives detection technology? What are other countries doing in this area, and how are we working with them to develop this technology?

Response: The S&T Directorate works with several key companies, academic institutions and others conducting research and development into explosives detection technologies. They include:

Aberdeen Proving Ground	Battelle
ACSA	Boeing
Analogic	Brigham & Womans Hospital

Questions for the Record
Senate Homeland Security & Governmental Affairs Committee
"After the London Attacks: What Lessons Have Been Learned to Secure U.S. Transit Systems?"
September 21, 2005
Assistant Secretary Kip Hawley

Creative Engineering Associates (CEA)
CyTerra
DESE Research
Duos
Eglin Air Force Base
FAA Imaging Technology Branch
Federal Aviation Administration
Galaxy
GE/Invision
General Electric
GST
HiTec
Hope College
INEEL
Johns Hopkins University
L3 Communications
National Institute of Standards and Technology
Naval Surface Warfare Center (NSWC)
Nomadics
Northrup-Grumman
Nottingham Trent University
Reveal
RMSC Columbia River
SAIC
Sandia National Laboratories
Sarnoff
Smith Detection
SRA
Suspect Detection Systems
Technical Support Working Group
TeraView
University of Central Florida
University of Illinois
University of Pennsylvania
University of Southampton
WeCU
Xintek

Questions for the Record
Senate Homeland Security & Governmental Affairs Committee
"After the London Attacks: What Lessons Have Been Learned to Secure U.S. Transit Systems?"
September 21, 2005
Assistant Secretary Kip Hawley

In order to accomplish its mission, the S&T Directorate and its Transportation Security Laboratory (TSL) engage in numerous international activities. International activities have taken many forms and include:

- Bilateral agreements with specific countries;
- Consultation on equipment certification and test and evaluation procedures;
- Participation in joint test and evaluation activities;
- Grants, contracts or agreements with foreign companies or universities;
- Assistance in the evaluation of foreign technology;
- Visitations by foreign delegations to the TSL;
- Visitations by foreign vendors to the TSL to discuss technology;
- Attendance by foreign vendors at TSL sponsored bidder's conferences;
- TSL sponsorship of international symposia; and
- Attendance by TSL personnel at international meetings and symposia.

Additional detail regarding grants, contracts, and agreements with foreign companies or universities; and assistance in the evaluation of foreign technology, follows.

❖ **Grants, Contracts, and Agreements with Foreign Companies or Universities**

Bulk Explosives Detection

Israel - Contract with Soreq – a government research facility – to develop detectors for gamma-ray resonant absorption;

Israel - Contract with Soreq – to develop sub-millimeter resolution frame-timed optical readout detectors for pulsed fast neutron transmission spectroscopy (PFNTS). For potential use in gamma-ray resonance absorption for EDS Cargo screening;

Germany - Contract with GE/Yxlon – to do research to improve performance of an X-ray diffraction-based explosives detection system. The system is being evaluated for use in alarm resolution; and

Australia – Contract with QR sciences – to develop a checkpoint screening system based on quadrupole resonance. TSL is funding modification of the signal processing.

Trace Detection

Japan – Cooperative Research and Development Agreement (CRDA) with Hitachi Ltd. – to evaluate a Mass Spectrometer Explosives Trace Detector. System has passed Laboratory certification, but has not yet passed Operation Utility Evaluation (OUE); and

United Kingdom – CRDA with MSA – for the evaluation of a trace boarding card

reader screening system.

Human Factors

Israel – Grant with WeCU Technologies Ltd. Caeseria – Cooperative Agreement #05-G-011 for Detecting Suspicious Behavior-Stimuli Research – for the evaluation of technologies to sense of individual's physiological responses and/or overt behavior that are associated with malicious intent. Examine pupil dilation, remote respiratory rate, remote heartbeat, and thermal facial measurements;

Israel – Grant with Suspect Detection Systems – Period of performance is one year. Evaluation of prototype system where candidate is hearing words and seeing words on a screen and is evaluated on his skin response and blood volume pressure. To be evaluated by Mosad in Israel, then in the United Kingdom and then in the United States by the National Safe Skies Alliance;

United Kingdom – Grant with the University of Southampton – Improving the efficiency of Visual Search;

United Kingdom – Grant with Nottingham-Trent University – Research grant; #04-G-020, Kinetic Depth X-ray (KDEX) Imaging for Security; and

Philippines – TBD – Evaluation of checkpoint security training and the possible use of Threat Image Projection.

❖ **Assistance in the Evaluation of Foreign Technology**

Advanced technology bulk detection system	Germany	Heimann Systems
Metal detectors	Italy	Ceia
Shoe scanning system	Israel	TBD
Mass spectrometer system	Japan	Hitachi

C. What is the current status of this research and development effort? When will the technology be ready for testing and deployment? Please provide a timeline for when you expect a breakthrough.

Response: The S&T Directorate is focused on the design, development and piloting of technologies and procedures to improve the ability to detect, interdict, and mitigate the effects of IEDs through a multi-phased life cycle R&D effort.

Explosives detection R&D for aviation security personnel and the aviation industry is involved

in short-term activities that include the evaluation of Commercial-Off-the-Shelf (COTS) and Non-Developmental Items (NDIs) and prototype devices to detect and incrementally increase our detection capabilities. Mid- and long-term activities will seek to develop greater capabilities for detecting aviation threats in checked baggage, passenger screening, air cargo and conveyance areas.

The IED Countermeasures Program is focused on the research, development, testing, and evaluation (RDT&E) of checkpoint, stand-off, and alarm resolution tools to detect suicide and vehicle bombs. Significant improvements over current detection capabilities (e.g., performance, reliability, standoff distance) require investment in new or improved technical capabilities, pilot demonstrations, and development of associated concepts for operation (CONOPS). Each of these efforts is pursued in a spiral development approach, i.e., capabilities improve with each iteration, and all successful developments are completed by piloting the systems in an operational environment with an associated CONOPs, protocols, and training package, i.e., a systems tool kit.

Suggestions for investment in RDT&E of new or improved technical capabilities for IED detection are being sought through various means, such as Broad Agency Announcements and the Small Business Innovative Research (SBIR) program. Technologies developed under this program will be demonstrated within the awarded contract, under pilot tests, and in conjunction with other departments or agencies.

A commercially available, vehicle-bomb-detection tool kit using a trace-detection system is planned to be completed by December 2006. Current efforts for the development of an automated-checkpoint system for detecting vehicle bombs are high-risk; however if successful, prototype systems may be available as early as 2008. Stand-off-vehicle-bomb-detection system development is in the research phase; a down-select of suitable technologies is not expected until 2009.

The development of suicide bomb detection systems is moving forward with a commercially available suite of technologies suited for a rail environment and associated tool kit slated to be available by December 2006. The planned development of stand-off, imaging systems will complete the prototype phase by 2008. In addition, the development of automated stand-off detection systems is currently in the research phase; a down-selection to suitable technologies is not expected until 2010.

The law enforcement community largely desires man-portable automated detection systems to support their current CONOPS. It is expected that a pre-production prototype hand-held radar system, used as an alarm resolution tool to screen people in secondary screening situations, will be piloted in a rail environment in September, and an associated tool kit completed by early 2007. Hand-held-trace-detection systems are currently in the development phase, and a prototype will be available for laboratory evaluation by 2007.

Questions for the Record
Senate Homeland Security & Governmental Affairs Committee
"After the London Attacks: What Lessons Have Been Learned to Secure U.S. Transit Systems?"
September 21, 2005
Assistant Secretary Kip Hawley

- **Defense Technologies**

2. The U.S. Department of Defense (DOD) has been investing millions of dollars in research to detect and defeat conventional explosives, such as systems to detect improvised explosive devices (IEDs) in Iraq. How do DHS personnel interact with the DOD IED Task Force, DARPA, the Combating Terrorism Technology Support Working Group (TSWG), and other defense organizations to leverage their research and development investments and make use of their technologies and advances?

Response: The S&T Directorate regularly communicates with the Department of Defense (DoD) and hopes to leverage their explosives and improvised explosives device (IED) research and development (R&D) to homeland security applications, including R&D strategy and systems development. However, because of different missions and often different threats, specific homeland security development is often required. Technologies employed as explosives countermeasures are not always appropriate for every operational situation or threat size and type even internal to the DoD and DHS mission spaces. Operational control, detection, and interdiction of devices in a combat zone, versus in a crowded public venue in a major metropolitan area, are very different and result in collaborative but distinct R&D efforts.

The S&T Directorate has co-sponsored R&D of IED detection technologies, shared test and evaluation data, and collaborated on R&D strategic planning to reduce duplicative efforts and shorten the development cycle across the Federal government. Examples include; the development of a stand-off vehicle bomb system with the Army Research Laboratories; the development of a hand-held suicide bomb detection system with the Technical Support Working Group (TSWG); the development of an RDT&E explosives countermeasures strategy with the Office of the Deputy Under Secretary of Defense (DUSD) Advanced Systems and Concepts; and the development of an RDT&E blast mitigation strategy with the U.S. Army Corps of Engineers. The S&T Directorate currently collaborates with:

- Office of the DUSD, Advanced Systems and Concepts
- Technical Director, Joint IED Defeat Office (JIEDDO)
- Joint Lab Board, Joint IED Defeat Office (JIEDDO)
- Technical Support Working Group (TSWG)
- Office of the Chairman, Physical Security Equipment Action Group (PSEAG)
- Naval Explosive Ordnance Disposal Technology Division
- U.S. Army Corps of Engineers
- U.S. Army Research Laboratories

- **Evaluating Technologies**

3. Local officials and transit agencies considering investments in new detection technologies need to evaluate a variety of systems offered for sale by contractors.

A. What is your understanding as to how local officials and transit agencies typically go about getting detection technologies tested and technically evaluated?

Questions for the Record
Senate Homeland Security & Governmental Affairs Committee
"After the London Attacks: What Lessons Have Been Learned to Secure U.S. Transit Systems?"
September 21, 2005
Assistant Secretary Kip Hawley

Response: In general, local officials tend to be highly reliant upon the manufacturers' claims of performance and applicability. In addition to such information, there are reports in the public domain regarding testing of commercial items that can be accessed, though the reports may require interpretation. Often, Federal agencies pursue transit agencies and state and local communities to support the evaluation of technology within an operational environment, such as a mass transit station. In these cases, local officials and transit agencies have access to the data collected in their specific environment.

The Office of Grants & Training (G&T) in DHS coordinates an interagency group responsible for the development of an approved equipment list (AEL). Additionally, G&T evaluates equipment against user requirements. When data is available, the interagency group uses this data to support the addition of equipment to the AEL. The Environmental Protection Agency (EPA), through its Environmental Technology Verification Program and its derivative Technology Test and Evaluation Program, also generate reports that provide some guidance. These programs tend toward validation of manufacturers' claims and are not necessarily directed toward developing a full and fair assessment of all available technologies.

Testing and evaluation and technical assessment programs for specific categories of homeland security technologies that are offered for sale to local and transit officials are currently underway in several components of DHS as well as in other Federal entities including the Department of Defense, the Technical Support Working Group, and the National Institute of Justice. Results of many of these tests (of equipment on the AEL) are available to public sector officials through the Responder Knowledge Base (www.mipt.rkb.org), which is maintained by G&T.

B. Does the federal government provide technical assessments or testing for systems that may be offered for sale by contractors to local officials and transit agencies? Does the federal government provide any sort of "seal of approval" for effective technologies and systems that can help local governments make cost effective procurements.

Response: Testing and evaluation and technical assessment programs for specific categories of homeland security technologies that are offered for sale to local and transit officials are currently underway in several components of DHS as well as in other federal entities including the Department of Defense, the Technical Support Working Group and the National Institute of Justice. Results of many of these tests [of equipment that is on the DHS Office of Grants and Training's (G&T) approved equipment list (AEL)] are available to public sector officials through the Responder Knowledge Base (www.mipt.rkb.org), which is maintained by G&T. The Responder Knowledge Base provides information on what generalized items (on the AEL) can be purchased with grant funds and provides links to related products via the Interagency Board (IAB) Standardized Equipment List.

There is no formal federal seal of approval, but DHS does follow the guidance of the National Technology Transfer and Advancement Act (NTTAA) (PL 104-113, 1995) and promotes the

development of voluntary consensus standards for homeland security equipment. These standards are reflected in the annual DHS grants guidance provided to state and local governments.

More specifically, the S&T Directorate is currently engaged in developing equipment standards for personal protective and operational equipment; chemical, biological, radiological, nuclear and explosive (CBRNE) detection and decontamination equipment; and mitigation technologies for use by the public and private sector, including local officials and transit agencies. Nineteen Standards Subject Area Working Groups have been established within the S&T Directorate to review and deliberate technical discussions within each of the aforementioned categories. Each of the working groups is composed of partnerships which engage experts from the Federal, state, local, and private sector communities. The S&T Directorate works with these partners to discuss relevant criteria, and thereafter develop, adopt, and publicize equipment standards. Of the 21 equipment categories specified in the AEL, four correspond to the equipment standards subjects deliberated by the S&T Directorate. Standards adopted by the S&T Directorate within those four categories are thereafter reflected in the G&T AEL. Doing this ensures that grantees are mandated to comply with procuring equipment that meets those standards.

Statement of
Mike Brown
Chief Operating Officer
London Underground
September 21, 2005

London Underground – Background Information

London Underground (LU) is the world's oldest underground railway network. The first section opened between Paddington to the east and Farringdon Street – near to the business district "City" of London in 1863. There are 253 miles of route, 45% of which is in tunnel. Track voltage is 630v DC (4 rail system). There are 273 stations served by Underground trains, and of these 255 are operated by LU.

London Underground provides a public transport railway service to London. It is part of Transport for London, a public transport authority under the direct control of the elected Mayor of London.

Approximately 3 million passenger journeys are undertaken each day on the Underground network – roughly the same number as on the whole of the rest of the rail network across the United Kingdom.

The busiest staion on the Underground network is Victoria with 75.6 million passengers per year. 150,000 people enter the tube system every hour.

Some 6000 staff work on stations. All stations on the network have a staff presence and larger locations in Central London will have 20 or more staff on shift at any one time, assisting with train dispatch, safety & security and customer information.

Operation

In November 2003, London Underground reorganised its operational structure to focus around each Tube line under the overall leadership of Managing Director Tim O'Toole.

The new structure is headed by Chief Operating Officer, Mike Brown, who is reported to by three Service Directors. Each Service Director is responsible for a grouping of lines which are maintained and improved by a separate Infrastructure Company.

Under the Service Directors are ten line General Managers each responsible for running and improving performance on their line, covering both trains and stations.

While the line General Managers concentrate on the day-to-day running of the service, the Service Directors look at long-term development and overall network performance. They are out and about on the network understanding the complexities and issues unique to each line.

The Public Private Partnership established by the Central UK Government, has set up three private sector consortia to take responsibilty for the maintenance and renewal of the track, infrastructure, trains, signals and other assets, while London Underground is responsible for the operation of these contracts and for the operation of the system.

In addition to the funding this generates, the Mayor of London and Transport for London have secured additional investment for capital programmes in the Underground.

The Security Situation before 7th July 2005

CCTV - the London Underground system has over 6000 cameras on nearly all stations and in trains.

620 Police officers are permanently assigned to London Underground.

6000 front line station staff are deployed across the Tube's Stations. These staff work either on platforms, at ticket barriers, in local station control rooms or on patrol across one or more stations.

All trains have a driver in the cab, who is in contact by radio with a line control centre (there are 7 such rooms across the network.)

The majority of attacks before July 7th were carried out by Irish republican terrorists, who had been involved in terrorism in all parts of the UK (not just Northern Ireland); who usually (although not always) gave a warning prior to their bombs exploding.

The bombings of 7th July were unprecedented in terms of the numbers of people killed and injured in the United Kingdom railway attacks. Prior to that date, most attacks had been designed to disrupt or damage assets rather than cause mass loss of life.

The Underground is an environment where the millions of people conveyed each day have no full check on their identity. No screening of their possessions take place and there are only ticket gates to control movement in and out of the system.

The phenomenon of the suicide bomber means any traditional measures of detection and interception is likely to be ineffective. Here effective response to an incident is the key.

The so called HOT principle is used by London Underground Staff and the police to manage unattended items discovered at Railway stations. The use of these protocols has saved the London Underground system from a large number of closures over many years, as there are typically over 300 items left on the network each day.

H - Is the item hidden, or concealed from view? – explosive devices are not usually left in an obvious place because of the risk that they will be detected before exploding. Fear of failure is the biggest factor for a terrorist.

O – Is the item obviously suspicious – does it look like a bomb (wires, power supply or other elements to indicate it may be a device.)?

T – Is the item typical of what might be expected at a particular location? – for example genuine lost property is often found in a place where people have been queuing or congregating before moving on to another location.

The success of this protocol on the Underground system has significantly reduced the number of security alerts where the system has had to close whether fully or in part. It is our belief that these protocols remain relevant for unattended items – although not in the case of a suicide attack.

After the 9/11 attacks in the United States of America, London Underground played a full part in the resilience planning process put in place by the UK Government and supported by the Mayor of London. There has been a manager seconded to the London Resilience team (LRT) since it was established and this has ensured that the operational realities of a mass transport metro system can be properly considered in political and investment decisions.

This team has led work in areas such as evacuation of parts of London, chemical, biological and radiological attacks and, most visibly has arranged table top and live emergency exercises. The largest of these was a weekend exercise at Bank London Underground Station which simulated a chemical attack at one of the largest, most complex stations on the network. This was a multi agency exercise which was also attended by political leaders.

The learning from all exercises played a vital role for Underground senior managers in revising training and in their own actions on July 7th.

The LRT also enabled the joint development of a battery powered track trolley – designed to enable emergency service personnel to travel down the tunnel to an incident train while wearing their heavy and cumbersome protective suits. Although the events of July did not require such protective suits to be worn these trolleys were deployed to help with casualty and later with body recovery.

As well as these larger scale exercises, London Underground arranges every year a smaller scale live incident - again with the co-operation and involvement of the police, fire and ambulance services. While these exercises cannot involve all members of staff who might benefit from such practical training, they do present a very real scenario for the senior and middle management team to experience and to learn lesson from.

In March 2004 London Underground hosted a security conference in London for key personnel from other transport operators across the world. There were representatives from the USA, Russia, Israel, Spain & France – all of who had suffered from terrorist attacks. With unfortunate irony, the attacks on Madrid happened during this conference.

A further security conference is being arranged in London this autumn sponsored by UITP (International Association of Public Transport) and hosted by Transport for London.

Events of July 7th

At 08.49, 3 explosions happened simultaneously and without warning across the Underground network. 2 of the explosions were on trains on the Circle Line; one as a train had just left Edgware Road station to the west end of London on its way to Paddington. This train was passing another (Eastbound) Circle line train at the time as the bomb exploded. The other bomb on the Circle line exploded on a train which had just left Liverpool Street station on its way to Aldgate.

The third explosion took place in the narrower, deep level, Piccadilly line on a train which had just departed King's Cross St Pancras station on its way to the next Station, Russell Square. The tight, deep level tunnel, led to a higher number of deaths and serious injuries here than elsewhere.

At 09.47 a further bomb exploded at Tavistock Square on a bus. This was very close to the Russell Square incident.

In total 38 people were murdered on the Underground – 7 at Edgware Road; 7 at Liverpool Street and 24 at Russell Square. 700 people were injured. Also 14 people were killed on a bus at Tavistock Square.

For upwards of half an hour London Underground Staff were the first responders to the incidents. Station staff, train drivers based at Edgware Road, cleaners and a large number of managers recovered the dead and the dying in horrific circumstance at all sites. The drivers of all 4 trains (2 involved at Edgware Road) were among the many that performed with amazing courage, dedication and compassion for several hours.

As it became clear as to the scale and nature of the incidents, the entire Underground system was evacuated. This followed a well rehearsed plan and ensured that apart from one train (stuck behind the one that exploded at Russell Square , the entire system was evacuated of over 200,000 people in less that one hour after the call was made to evacuate. This was a remarkable achievement especially as the capacity of the mobile (cell) phone network was unable to cope with the volume of calls being made by members of the public.

During the day, the emergency services took full control of the 3 sites while London Underground began to plan for recovery. Trains were moved back to the depots in the unaffected parts of the network and less than 24 hours after the incident, the entire rest of the network was operational.

Recovery of the network

In accordance with our contingency plan, a recovery team was established led by a Service Director. This role was to ensure that working with the police all evidence was gathered as required but that the imperative for service restoration was also made. It was also vital to ensure that all engineering repair resource was able to be deployed immediately as the sites were released by the police.

Trains ran through Aldgate on 25th July. The Edgware Road section resumed on 29th July and the Piccadilly line resumed through Russell Square on 4th August – 4 weeks after the explosion.

It is worth pointing out that the rapid restoration of 80% of the service - less than 24 hours after the explosions gave confidence to London and the UK overall.
As of mid September 2005, passenger numbers are at the same level as they were in 2004.

The new normality

Operational issues

On 8th July, all staff were put in high visibility orange vests across the network. In addition all managers with any operational experience were deployed across the network and also asked to wear orange vests.

Police deployment was unprecedented with major patrols at the main central London Stations and over the next weeks there would be occasions when every station on the Tube network had at least 2 police officers deployed, through the operational day – in addition to regular station staff. 100 extra police officers have been funded by London Underground and are now being recruited – bringing the total to 720.

Enhanced staff briefings were instigated to ensure that train drivers and station staff had rapid access to information as it unfolded. This proved to be particularly important on the 21st July when 3 bombs failed to detonate on the Tube, but where the system was kept operational as we were able rapidly to communicate to all staff as to what had happened. It was the positive attitude which enabled the network to recover so quickly.

17,000 CCTV tapes were removed by the police immediately after the event of July 7th and it was vital that these tapes were replaced. This happened following a protocol which might normally only apply to one station or train. This was a significant challenge as the protocol only envisaged for no more than one day.

All stations and trains have public address systems and after the 7th July this was used to consistently give out security messages. It was also vital as a way of reassuring passengers as to the fact there were staff throughout the network concerned for their safety and security. London Underground senior managers had briefings at the highest level from the UK Government and/or the senior ranks of the police on at least a daily basis.

The criticality of the radio system has become even more obvious since the bombings. Although all radio communication did work (except for the incident trains) during the incidents, it has become clear since then that there are some weak areas of reception and transmission. Those parts of the network not above ground do not have access to the mobile (cell) phone network and therefore rely heavily on the operation of the radio infrastructure.

The existing plan to renew the radio system across the network has been revised and brought forward so that all lines will have a new radio system in place by the end of 2006. In the meantime additional hand held radios have been purchased to supplement the units fitted to each driving cab. Also on open sections of the railway (above ground) other conventional radios have been deployed to enable operation in the event of a failure in these areas.

However, in the meantime, the operational procedures of the Tube have been changed so that if the radio is inoperative (no transmission or reception between the train and the control room), passenger service will now be suspended.

Investment and Funding of security on the Underground

Prior to the 7/7 attacks London Underground were working on an agreed Security Improvement Programme. The project team assigned to this has now widened its remit to take on board lessons learnt from 7/7.

Overall investment in London Underground over the next five years will be £5.5 billion. This reflects both the London Underground directly managed investment, together with the capital works delivered through our Public Private Partnership and Public Finance Initiative contractors.

The Public Private Partnership arrangements are an integrated, upgrade and maintenance investment which have many security enhancements as part of their works.
At least £70 million of the Public Private Partnership works will be spent on safety and security related improvements over the next five years (does not include all station works as these are integral to the wider modernisation programme).

London Underground investment includes work on enhancing CCTV prior to the planned Public Private Partnership modernisations and refurbishments. Since 7th July following a review there are currently plans to accelerate delivery of these works over the next 6 months.

Other London Underground works include improvement to communications via station and train radio. Also to allow emergency services to use their radio systems underground. The day to day spend for security and British Transport Police has been enhanced allowing recruitment of an extra 100 Police Officers. The annual policing cost for London Underground Ltd ongoing is £50 million. To support the police and security of London Underground costs a further £10 million. There has been an increase since 7/7 of roundly 10% of operational cost for safety and security measures.

The Future

London Underground will continue to work with the UK Government and other world wide agencies as technology improves in the fight against terrorism. Although there have been a number of trials of various detection and other portable and fixed devices across the world, it is not yet clear whether these justify the considerable investment and maintenance required. Also and more importantly, it is not yet clear whether these devices will effectively deter against a number of different risks - rather than lead both public, transport operator and police into an unrealistic state of feeling more secure. Clearly London Underground needs to be clear about the objective of installing new technology and clearly understand the real benefits.

Incident Review

As the network returned to normal it became obvious that there should be a full review of all lessons learnt form the events. This is not yet in its final draft; however there are a number of things which have emerged already and which will require further review. These include:

Car design:

As part of the full review of the events in July, there has been some feedback that the location of rails and grab poles in cars may have caused difficulty for some of the immediate rescue and recovery operation.

Staff Training:

Operational training is undergoing a full structural review within London Underground. This review will include the level of practical rescue and recovery training given to existing drivers and station staff. Already all staff on the underground undergo 5 full days refresher training every year. The content and duration of this is being reviewed.

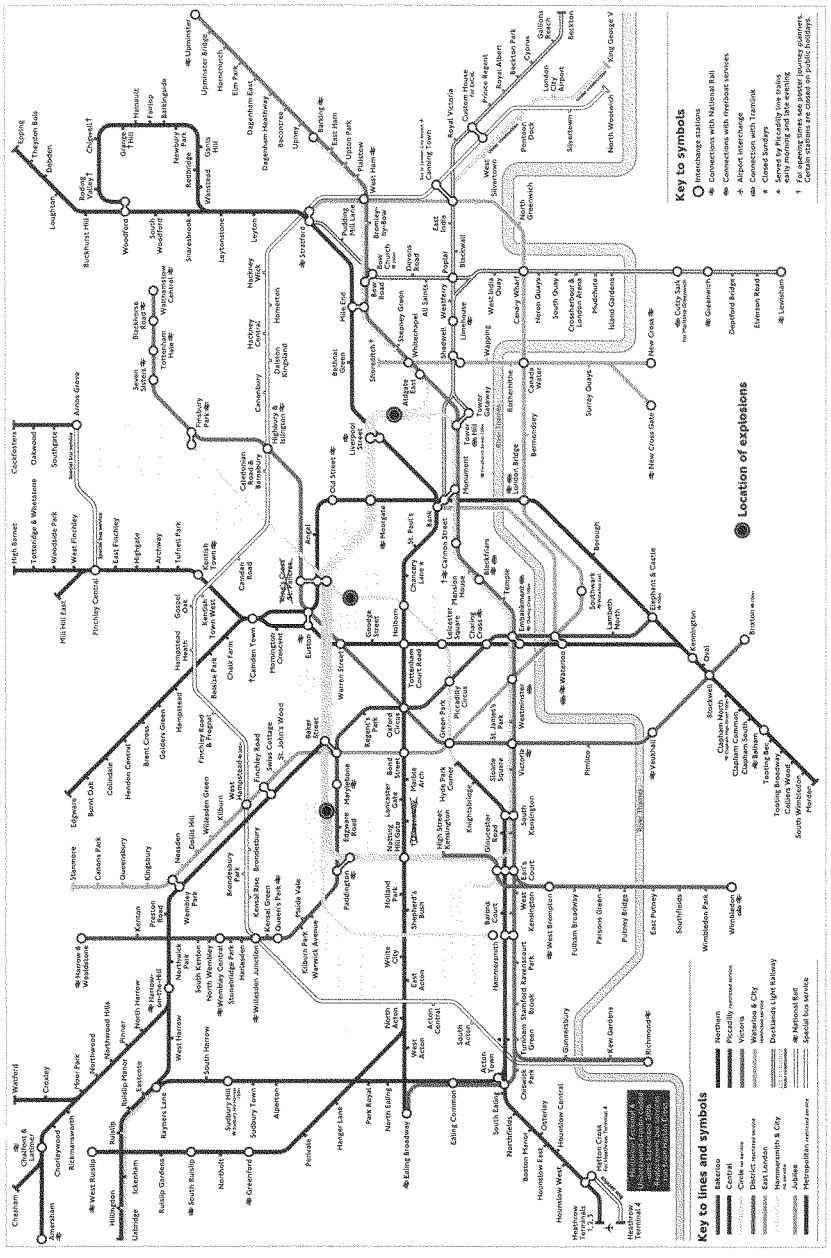
Resources:

With 3 incidents sites and then further incidents on the 21st and 22nd July, there were times when the recovery and operations teams were fatigued. In future a planned phasing of rest periods will be implemented to ensure resource is available in a fit and healthy state at all times in a 24 hour period.

Multi site incident management:

Lessons were learnt regarding the management of multiple incident sites; mainly concerning the co-ordination and integration with the emergency services.

Mike Brown
Chief Operating Officer
London Underground Limited


Location of explosions
Key to symbols
Interchange stations
Connections with National Rail
Connections with riverboat services
Airport interchange
Connection with Tramlink
Closed on Sundays
Served by Piccadilly line trains early morning and late evening
† For opening times see zonal journey planners. Canary Wharf and Canada Water stations are closed on public holidays.
Key to lines and symbols
Bakerloo
Central
Circle
District
Hammersmith & City
Jubilee
Metropolitan
Northern
Piccadilly
Victoria
Waterloo & City
Docklands Light Railway
Tramlink
National Rail
Special bus service
© Transport for London

STATEMENT OF POLLY HANSON
CHIEF
METRO TRANSIT POLICE DEPARTMENT
WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS
UNITED STATES SENATE

SEPTEMBER 21, 2005

Chairwoman Collins and Members of the Committee, good morning and thank you for asking me to testify on Washington Metropolitan Area Transit Authority's (WMATA) security initiatives. I am Polly Hanson, Chief of the Metro Transit Police Department (MTPD for WMATA.

By way of background, WMATA was created in 1967 as an Interstate Compact agency through enactment of legislation by the U.S. Congress, and by the Commonwealth of Virginia, the State of Maryland, and the District of Columbia. The Metro System was designed to serve the constituencies of the National Capital Region, including employees of the federal government, the residents of the region, the citizens of our nation who come to Washington to do business with the federal government, and the millions of people who visit from throughout the world.

Since the mid 1960's, there has been dramatic growth and change in the National Capital Region. As population and employment in this region has skyrocketed, the demands on and expectations of WMATA have also grown exponentially. Each day we provide 1.2 million trips on our rail and bus systems. We are the second largest subway system and fifth largest bus system in the United States. Metro is widely recognized as being critical to the operation of the federal government. Over 150,000 federal employees (45 percent of the region's federal employees) participate in the Metrochek program. Nearly half of all Metrorail stations serve federal facilities, approximately 10 percent of Metro's daily ridership uses stations next to the Capitol and Pentagon.

The Metro Transit Police Department was established in 1976. MTPD is the nation's first non federal tri-state transit police force. We have authorized strength of 400 sworn transit police officers and 101 special police officers. Our purpose is to prevent crime, protect Metro's customers, employees, facilities and revenues and enforce laws, ordinances, rules and regulations.

As the largest transit provider for the National Capital Region, Metro takes its responsibility in homeland security with the seriousness it demands. WMATA's approach to transit security involves a partnership between employees, customers, the transit police and other public safety departments in the region, and the federal government. It's a strategic approach that merges the application of technology with enhanced operational awareness, and puts an emphasis on training, public outreach campaigns, and the use of security assessments that take into consideration the unique designs of transit. Working in partnership with the American Public Transportation Association (APTA) and other transit systems across the country, WMATA has assisted in the development and is utilizing many of the industry's best practices to implement this strategy.

Security Actions Taken Before and After September 11, 2001

WMATA has been hailed by some as a "national security asset" both for its efficient performance on that fateful day of September 11, 2001, and for its potential

future role in serving the National Capital Region during a major regional incident or emergency situation. WMATA had spent considerable time and resources on emergency preparedness even before September 11th. In the aftermath of the 1995 nerve gas attack in the Tokyo subway, we began in partnership with the Departments of Energy, Transportation, Justice, and the National Laboratories to develop a chemical sensor detection system for use in a transit environment. Metro's chemical detection system, which is now fully operational, has become a model for other transit agencies across the nation and around the world.

Also prior to 9/11, WMATA's transit police and safety departments had prepared System Safety and System Security Program Plans, established procedures and practices for activating our Emergency Operations Command Center, conducted annual counter-terrorism and explosive incident training for police and operations personnel, as well as providing a high level of interagency coordination and training programs and exercises with the many law enforcement and fire and emergency rescue agencies in the metropolitan area.

Since 9/11, WMATA has undertaken a number of additional actions to enhance our security and emergency preparedness. With $49 million of funds made available by Congress after the attacks, WMATA undertook a number of initiatives, including:

- Advancing the chemical sensor detection system from the testing and pilot to the operational phase
- Installing intrusion detection capability and ID entry system at WMATA employee buildings, facilities, and stations
- Installing Automatic Vehicle Locators on Metrobuses
- Equipping a portion of Metrobuses with digital cameras and recording capability
- Installing bomb containment trash cans
- Purchasing Personal Protective Equipment and additional K-9 teams for transit police and
- Putting in place an alternative command center and interim backup operations control center capability
- Initiating the installation of redundant fiber optic infrastructure to ensure emergency communications.

The early warning data flowing from the chemical sensor detection system, commonly referred to as "PROTECT," is fully integrated into our Operations Control Center and critical real-time information and live images can also be accessed at safe zones for use by incident commanders responsible for responding to an event.

WMATA has also been subject to two comprehensive external security assessments since September 11, 2001. The Federal Transit Administration completed a threat vulnerability assessment in the spring of 2002, and DHS's Office for Domestic Preparedness conducted a risk-based security needs assessment in 2004. Both assessments cited the need for redundancy in key operations control and communications systems as a top security priority for WMATA.

Madrid and London Bombings: A Heightened Level of Awareness

The actions taken in response to the terrorist attacks in Madrid last year and London in July are designed to enhance both WMATA and the region's emergency preparedness.

MTPD Actions

Actions taken by the Metro Transit Police Department (MTPD) include:

- Purchase of additional explosive ordinance detection equipment
- Increasing the frequency of station patrols by transit police special response teams (similar to SWAT teams) who patrol with specially trained explosive detection canines and machine guns
- Altering the way in which transit police are conducting sweeps of trains and increasing the number of police officers patrolling during rush hour
- Metro Transit Police receive regular updates from the FBI and the region's chiefs of police and a member of the Metro Transit Police has been selected to represent the entire transit industry on the FBI's National Joint Terrorism Task Force
- Additional security measures that are not visible to our customers and are designed to be that way
- Purchase of additional radiological pagers for use on patrols
- Created a multi-jurisdiction partnership with other local police departments to assist with rail station and bus sweeps

Increasing Public Awareness

A critical component towards raising the nation's emergency preparedness level is to also constantly engage the public. WMATA has increased public announcements to our customers, stressing the need to be attentive to their surroundings. Our recent public outreach efforts include campaigns known as, "See it, Say it" and "Hey, Is that your bag?," which was cited by former Department of Homeland Security (DHS) Under Secretary Hutchinson as an effective tool for raising passenger awareness and involvement in the transit environment.

September is National Emergency Preparedness Month and WMATA has been sponsoring numerous outreach events to our customers. WMATA hosted an information booth and conducted K-9 unit and rail emergency evacuation demonstrations at the September 1st DHS kick off event at Union Station. Our safety office has been offering emergency preparedness seminars at the offices of large regional employers. We are also conducting "Open Houses" at major rail stations every Tuesday and Thursday during the month of September. During these events, officials from the Metro Transit Police and our safety and communications departments are on hand to answer questions from customers as well as distribute emergency preparedness brochures and expand upon emergency evacuation procedures and alternate route planning that can be found at or web site: *metroopendoors.com.* WMATA is also an active participant in the NCR's Emergency Preparedness Campaign, including assisting in the creation of handy information cards, known as "Z cards" and by providing free advertising space

throughout the system to promote greater public involvement on the emergency preparedness front.

Training our Workforce and the Region's First Responders

The recent events in London have also called for a top to bottom re-emphasis and re-energizing of our entire workforce on anti-terror and emergency response training. Since 2003, all of our bus drivers, train operators and other operations employees have been shown the National Transit Institute's *Warning Signs* video, which covers key aspects of system security for transit employees, including what to look for and what to do regarding suspicious activity, packages, devices and substances. In August, we began showing the video again to all of our 8000 operations employees. They also receive job specific security brochures covering these areas. The *Warning Signs* video is also being shown to non-operations personnel, and has been posted on our internal web site for viewing by all 2000 non-operations employees.

We are supplementing our existing training for both operations and non-operations personnel with additional terrorist activity recognition and reaction training classes. On the operations side, WMATA is working with the National Transit Institute to specialize the training to address the diverse responsibilities on the operations side that includes functions beyond bus and train operators, such as the maintenance of the escalators, track structures, buses and railcars. The training will include hands-on scenarios in recognition, decision-making, and demonstration of procedures covering situations like unattended or suspicious items and unusual behavior.

All of this training will serve to reinforce the need for our employees to respond aggressively in these situations, but it's also worth noting that our operations employees on a daily basis face the challenging task of keeping a prudent balance between implementing proper security safeguards and maintaining rapid transit service.

We also continue to enhance and extend our training partnerships with the region's first responder community and the Department of Homeland Security. Just this spring, Metro Transit Police launched a new training initiative entitled "Managing Metro Emergencies." The training was devised and developed in response to the Madrid bombings as well as a recent series of service disruptions that forced thousands of customers to evacuate the Metrorail system. The "Managing Metro Emergencies" course is providing approximately 1,500 regional law enforcement, fire and rescue, department of transportation and WMATA personnel enhanced training for mitigating, evacuating, transporting and recovering from a major service disruption in our system.

Last year, Metro Transit Police launched a Metro Citizens Corps program that provides Metro-specific training ranging from rail safety and emergency preparedness and response to identification of terrorist activity. Citizen participation initially consists of Citizen Emergency Response Teams (CERT) already organized in the District of Columbia, suburban Maryland and Northern Virginia.

Metro Transit Police are also currently working on expanding a partnership with DHS that began during this year's presidential inauguration to offer advanced behavior assessment training to the region's law enforcement community. In accordance with HSPD-5: Management of Domestic Incidents, Metro Transit Police officers have been National Incident Management System (NIMS) and Incident Command System (ICS) trained and certified, and we have started to expand the training to key management and operations personnel.

WMATA's Emergency Response Training Facility opened in 2002, and is the only transit facility of its kind in the nation that is available 24 hours per day, seven days a week to train emergency personnel. The facility includes a mock train tunnel that allows regional emergency responders to train for disasters such as smoke/fire, collisions and potential terrorist incidents in a transit/tunnel environment. WMATA's emergency management team trains an estimated 2000 federal, state and local emergency personnel each year. The facility was awarded the American Public Transportation Association's Management Innovation Award for 2004.

Transit Needs Additional Federal Support From DHS

The Department of Homeland Security and Congress have yet to make the protection of transit infrastructure a top homeland security priority. Less than $250 million of grant funding over three years has been allocated nationwide to transit since the creation of DHS in 2003. That amounts to an average of less than 0.3 percent of DHS's annual budget of $30 billion, and prospects are not looking much better for the upcoming year. The catastrophic consequences of Hurricane Katrina, highlighted by the breaching of the levees in New Orleans, should serve as a stark wake up call to the dire implications of neglecting to take serious actions to protect and strengthen our nation's critical infrastructure.

Given the modest amount of federal support for transit security to date, the Office for Domestic Preparedness (ODP) within DHS needs to simplify the grant application process in FY2006 to ensure that already identified needs based on both external and internal security assessments can be addressed in expedited manner. Due to the numerous layers of coordination, planning and approval requirements associated with the FY05 transit grant program, most of which replicates what transit systems are already doing, we are now almost a year after enactment of the FY05 DHS Appropriations bill, and two months after the London bombings, and we still have not gotten the green light from DHS to spend our FY05 grant funds.

At the very least, for FY06, DHS should be able to evaluate all the risk assessment information submitted by transit agencies in the past years and provide specific allocations to each transit system based primarily on risk, rather than allocating funds on a regional basis. We do support ODP's regional focus, as reflected in the formation of Transit Security Regional Working Groups, for the purpose of improving coordination and information sharing between transit systems. Regional allocations,

however, results in needless delays, and opens the door for criteria other than the assessment of threats and vulnerabilities to play a prominent role in the decision making process for the distribution of funds within a region. DHS should also consider providing the funds directly to transit agencies, and cut-out the various middle men that are far removed from the daily operation and protection of transit systems.

Our industry has the experience and knowledge in transit operations and security. Transit systems around the country working in partnership with the American Public Transportation Association have played a leadership role in developing security related best practices and forums for the industry in areas such as intelligence sharing, system safety and security guidelines, employee training, emergency preparedness and prioritization of transit research projects. But the energy and ingenuity exhibited by the transit sector since the tragedy of September 11, 2001 four years ago must be matched by a greater commitment of resources and risk-based planning by DHS in order to enhance the security of the more than 32 million customers who ride our subways and buses each weekday. In doing so, DHS needs to more fully engage and work with the transit industry to ensure that programs are developed and implemented in a flexible and practical manner that takes into consideration the variations in transit systems across the country, which is an entirely different process compared to securing airports. DHS must also do a better job of coordination and information sharing among internal agencies within the Department, such as ODP, TSA, IAIP and the Science and Technology Directorate, with transit security responsibilities.

The transit community also needs DHS's help in the development of standards for detection/surveillance technologies and other security items applicable for target hardening in a transit environment. Currently, there are far too many companies knocking on our doors insisting that they have the perfect solutions for enhancing our security. We don't have the time and resources to sift through all the options out there and identify the systems that will best meet our needs.

As part of the "Metro Matters" capital improvement campaign launched in the fall of 2003, WMATA identified $150 million of high priority outstanding security needs. Yet, WMATA has received only a total of $15 million in DHS transit security grants over a three year period. WMATA has allocated most of these funds towards beginning to address the need for redundancy and enhanced reliability of key operations control and communications functions, which was highlighted as a top priority by both the DHS and FTA security assessments. Other high priority security needs on the capital side include enhancing current WMD detection capabilities, expanding intrusion detection and surveillance systems, enhancing decontamination response and recovery capabilities, upgrading the public address system, additional anti-terror equipment for the transit police and additional video cameras on buses.

WMATA's Partnerships with the Federal Government

There have been some positive developments in terms of our relationship building with the federal government I would like to take a moment to discuss our partnerships in

emerging detection technologies and security procedures that are applicable to the transit environment.

WMATA continues to serve as a test-bed for the federal government and model for the country on new transit security initiatives. Metro's chemical detector system, commonly referred to as "PROTECT," has become a model for other transit agencies across the nation and around the world. The early warning data flowing from PROTECT is fully integrated into our Operations Control Center and the data and live images can also be accessed at safe zones for use by incident commanders in the region responsible for responding to an event. Federal partners who worked with WMATA in the development of the PROTECT system include the Departments of Justice, Energy, Transportation and Homeland Security. Working with our federal partners, WMATA continues to offer training and technical assistance on the PROTECT system to interested transit systems in the United States and around the world. WMATA is actively engaging the Department of Homeland Security in efforts to leverage the advances obtained by the PROTECT program to other emerging applications in the chemical, biological and explosive detection areas.

In January of this year, Metro Transit Police and Department of Homeland Security's Transportation Security Administration (TSA) collaborated to enhance security at Metrorail stations and on trains during the days surrounding the presidential inauguration. The first of a kind partnership with TSA, which included the use of federal screeners equipped with explosive trace detection gear and canines teams supplementing Metro's teams of officers and explosive detection canines, performed without a hitch and can be applied to other special events across the country. We are also working with DHS on expanding the application and training of personnel in the area of behavior assessment screening of passengers in a transit environment.

Early in 2004, WMATA was one of the first transit systems to subject itself to a comprehensive security risk assessment offered by ODP's Technical Assistance Program. It was a useful tool, quantitative and scenario driven in nature, for evaluating and ranking gaps in our infrastructure protection and response capabilities. While the assessment process had yet to be refined to take into consideration some aspects that are also critical to transit, such as recovery procedures and the evaluation of in-direct threats, it represents the only example of a DHS agency approaching us with a well thought out risk based process for assessing our outstanding security needs. The ODP assessment team appeared receptive to our suggestions for improving the process, and we recommend that other DHS agencies with responsibilities for assessing transit security, such as TSA and the Information Analysis and Infrastructure Protection Directorate, work with ODP to enhance and expand the use of this risk assessment tool.

WMATA also has a long standing productive working relationship with the Federal Transit Administration (FTA) on a wide range of emergency preparedness initiatives linked to training and exercises. The FTA has provided WMATA and other transit agencies technical assistance and support for continuity of operations planning (COOP), emergency drills, ongoing security forums and research coordinated through the

Volpe Center, and emergency training through the Transportation Safety Institute. In the case of training, the relationship has been a two-way street, with WMATA providing the FTA with in-kind instructional support for rail safety and emergency management courses.

WMATA's Regional Coordination Efforts Since 9/11

As the recent tragic events in the Gulf Coast illustrate, considerable coordination and planning among the region's state and local government players, as well as the private sector is necessary in order to ensure that WMATA's own emergency preparations and security upgrades will provide benefits to the National Capital Region during an emergency. Using the Metropolitan Washington Council of Governments (COG) as its primary coordinating body, the region has made significant progress on the issue of regional emergency response planning and coordination. As the lead transit agency in the region, WMATA continues to work with the rest of our partners in the transportation and public safety community to refine the plans already in place by providing more specific guidance on emergency transportation protection measures, including moving evacuation plans to the operational phase and improving internal and external communications during regional incidents.

WMATA has been a regular participant in exercises and drills sponsored by DHS, COG and various local jurisdictions. We also have conducted our own table top exercises with all key regional players, including federal agencies, as part of an effort to enhance WMATA's continuity of operations plans (COOP).

WMATA also has a long standing positive working relationship with the region's other law enforcement departments and emergency management agencies. Officials from both the Metro Transit Police Department and our Emergency Management team are on call 24/7 to represent WMATA at the District of Columbia's EOC during an emergency. The collaboration is also highlighted by the assistance WMATA provides to the District during special events by making additional buses available to transport personnel and provide perimeter security, as well as the assistance the Metropolitan Police Department, the Capitol Police and other regional law enforcement agencies provide to our police force when we are at elevated alert levels.

Conclusion

It's important to stress that we are constantly re-evaluating our top security needs based on new threat information, updated external and internal security assessments and emerging technological innovations. WMATA will also continue to pursue partnerships with the Department of Homeland Security to serve as a test-bed for new national initiatives in areas such as biological and chemical detection and enhanced security procedures targeted to a transit environment. Finally, the tragic events in the Gulf Region resulting from the fury of Hurricane Katrina, serves to reinforce the importance and

WMATA's commitment to continue to work with all our regional partners to further enhance emergency preparedness in the National Capital Region.

I want to thank you Chairwoman Collins and the rest of the members of the Committee for the opportunity to present these remarks and for the support this Committee has provided to Metro over the years. I would be happy to answer any questions.

STATEMENT BY RAFI RON
TO THE SENATE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS
September 21, 2005

Mr. Chairman and members of the Senate Committee on Homeland Security and Governmental Affairs.

For the record, I am Rafi Ron, President of New Age Security Solutions, a Transportation Security Consultancy firm based in McLean, VA. This company was established in October 2001 following a request by the Massachusetts Port Authority (Massport) to provide it with professional support in developing and implementing a new security policy and program so as to elevate Logan airport to a leading position in airport security. Logan's achievements are widely recognized today by the Federal Government as well as by the aviation industry.

Before my involvement with Massport and Logan Airport I served as Director of Security at Tel-Aviv Ben-Gurion International Airport for a period of five years. In this position I was responsible for all aspects of the security operation, including planning, implementation and management. My previous security experience stems from over 30 years of work in security, intelligence and counterterrorism for the government of Israel.

For the last four years, my company has been involved in numerous transportation security projects in the US and abroad involving airports, seaports and ground transportation.

I would like to thank the Committee for inviting me to testify about Transportation Security.

Over the past fifty years or so it has become clear that transportation is a high-priority target for terrorists and terrorist organizations. Since transportation systems constitute a critical infrastructure without which our modern industrial societies cannot function, these systems are very likely to remain at the high-risk end in the foreseeable future. Key links in our transportation systems are vulnerable to attack, and the potential damage may cause a large number of casualties as well as long shutdowns which can lead to major system collapse with multiple economic and political repercussions. No other system combines such a high level of vulnerability with so many attractive goals for terrorists acting against the United States.

As a result of the 9/11 attack, aviation security has been given a great deal of attention and the achievements are impressive. In less than four years, the United States of America has set itself as the global leader in aviation security and has become the driving force in making the domestic and global aviation system safer. Unquestionably, American aviation has become a harder target for terrorists to hit.

For terrorists this means that in order to ensure the success of an attack on aviation they would have to meet much higher requirements than ever before in terms of effort and sophistication. Concurrently, the disruption of the global terrorist organizational structure by U.S. global war on terror is resulting in the shift of responsibility for initiating and executing attacks to local terrorist cells, as we have seen both in the Madrid and the London attacks. The resources needed to mount successful attacks on hard targets are less readily available to terrorists operating on the local level.

The important lesson to be drawn from this recent history of terrorist activity is that once high priority targets are made harder, terrorist effort tends to be diverted towards minor targets that are still perceived as being soft. Mass transit remains a vulnerable target, more difficult to protect because of its vast extension and accessible nature, because attacking it does not require extraordinary resources, and because technological solutions have only a limited relevance to its protection. The turning of terrorist attention to urban mass transit systems is thus an expected consequence of our success in other domains.

Implementing the aviation security model in the mass transit environment is not an option. 100% screening cannot be performed with the technology available today without creating a bottleneck at check points. However, bottleneck check-points are not a proper solution because we need to allow high throughput without which mass transit cannot fulfill its role.

The challenge facing us is to develop a system-approach solution that combines technology, human resources and procedures. This system-approach solution must be designed to address the three stages of the security process:

- Preparedness and routine management
- Incident management and first response
- Recovery

The system must have an "open architecture" that will allow the shift of weight from one element to the other as more advanced and relevant technology becomes available and operational.

At present, the most relevant available technology is in the video field. Traditionally, video systems are installed in the location of the expected crime scene. While this is an effective way to identify criminals and secure the necessary evidence to convict them in court, it is totally inadequate to deal with a terrorist attack, because in the latter case, as soon as the attack takes place terrorist success has been achieved and the damage has been done.

What we need is a new approach to video application as well as to overall security planning. Prevention and deterrence must be the goal rather than detention and conviction. This distinct goal dictates pushing the security measures to the perimeter of the mass transit system. Our focus must be on detection and response **before** the terrorist gains access to the target. In other words, we need to shift our efforts from the train and ramp to the station entrances.

While video technology is undoubtedly important, it does not provide us with the most critical information we need – explosive detection. At present, explosive detection systems (EDS) are designed to meet the requirements of the aviation industry, and are not applicable in the mass transit environment. With research and development that recognizes this need and is focused on operational application, such EDS solutions can be available in the next couple of years. Current ideas in this area vary from air sampling techniques to trace detection on tickets or body parts that come into contact with the system in the entry process.

Appropriate technology is a critical factor in the protection of mass transit systems, but no technology can provide a solution without human individuals who can not only operate it effectively but also provide appropriate immediate response. It is useless to detect an explosive device if you cannot act to stop the person who carries it from entering the system.

Human resources will thus remain a critical element even when we have these future technologies at hand. At the present time, while these technologies are still in the works, the importance of the human factor is even more critical. In Israel, as well as in other parts of the world, the presence of trained security personnel at entrances of public facilities has proven to be a very effective preventive measure against terrorist attacks, including suicide attacks. Despite numerous attempts by suicide bombers to enter shopping malls in Israel, none has been successful. The terrorists were forced to carry out their attack outside the mall, the targets affected have been relatively minor and the damage sustained was smaller in terms of human life as well as property.

In reference to the human factor I would like to point out that the Achilles heel of the suicide terrorist is his behavior. A person intending to commit an extreme act of violence, in most cases for the first time in his/her life, as well as to terminate his own life is most likely not to behave like the ordinary people around him going about their daily routines. A signal example is Richard Reid (the "shoe bomber"), who was clearly detected by both security and non-security personnel as a suspicious person before and during boarding AA flight from Paris (Dec. 2001).

Behavior Pattern Recognition techniques implemented by trained security and non-security personnel have proven to be a valuable measure in the detection and prevention of terrorist attacks in public facilities. The training provides the skills and confidence not only to law enforcement officers positioned at entry points, but also to employees who are present at every point in the system. No one is in a better position to recognize irregularities on the ground than the people who regularly work there.

Let me sum up by reiterating three major points:
1. Legacy security programs in mass transit systems must be reassessed in light of the shift from the threat of conventional crime to the threat of terrorism, including suicide terrorism. This means putting a higher focus on early detection and prevention.
2. There is a pressing need to invest in technological R&D that will result in effective early detection of explosives and chemo/bio materials without disruption of throughput.
3. Security and non-security personnel in mass transit should undergo counter-terrorist training that includes suspicious behavior recognition techniques.

I thank you for your attention and I will be happy to answer any questions.

○