

3-1-2007

## The Fourth National Security Summit: Approaches to Passenger Screening, MTI S-08-01

MTI

Follow this and additional works at: [https://scholarworks.sjsu.edu/mti\\_publications](https://scholarworks.sjsu.edu/mti_publications)



Part of the [Transportation Commons](#)

---

### Recommended Citation

MTI. "The Fourth National Security Summit: Approaches to Passenger Screening, MTI S-08-01" *Mineta Transportation Institute Publications* (2007).

This Report is brought to you for free and open access by SJSU ScholarWorks. It has been accepted for inclusion in Mineta Transportation Institute Publications by an authorized administrator of SJSU ScholarWorks. For more information, please contact [scholarworks@sjsu.edu](mailto:scholarworks@sjsu.edu).



# The Fourth National Security Summit: Approaches to Passenger Screening



**MTI**

Mineta  
Transportation  
Institute

Created by  
Congress in 1991



# MINETA TRANSPORTATION INSTITUTE

The Norman Y. Mineta International Institute for Surface Transportation Policy Studies (MTI) was established by Congress as part of the Intermodal Surface Transportation Efficiency Act of 1991. Reauthorized in 1998, MTI was selected by the U.S. Department of Transportation through a competitive process in 2002 as a national “Center of Excellence.” The Institute is funded by Congress through the United States Department of Transportation’s Research and Innovative Technology Administration, the California Legislature through the Department of Transportation (Caltrans), and by private grants and donations.

The Institute receives oversight from an internationally respected Board of Trustees whose members represent all major surface transportation modes. MTI’s focus on policy and management resulted from a Board assessment of the industry’s unmet needs and led directly to the choice of the San José State University College of Business as the Institute’s home. The Board provides policy direction, assists with needs assessment, and connects the Institute and its programs with the international transportation community.

MTI’s transportation policy work is centered on three primary responsibilities:

## Research

MTI works to provide policy-oriented research for all levels of government and the private sector to foster the development of optimum surface transportation systems. Research areas include: transportation security; planning and policy development; interrelationships among transportation, land use, and the environment; transportation finance; and collaborative labor-management relations. Certified Research Associates conduct the research. Certification requires an advanced degree, generally a Ph.D., a record of academic publications, and professional references. Research projects culminate in a peer-reviewed publication, available both in hardcopy and on *TransWeb*, the MTI website (<http://transweb.sjsu.edu>).

## Education

The educational goal of the Institute is to provide graduate-level education to students seeking a career in the development and operation of surface transportation programs. MTI, through San José State University, offers an AACSB-accredited Master of Science in Transportation Management and a graduate Certificate in Transportation Management that serve to prepare the nation’s transportation managers for the 21st century. The master’s degree is the highest conferred by the California State University system. With the active assistance of the California Department of Transportation, MTI delivers its classes over a state-of-the-art videoconference network throughout the state of California and via webcasting beyond, allowing working transportation professionals to pursue an advanced degree regardless of their location. To meet the needs of employers seeking a diverse workforce, MTI’s education program promotes enrollment to under-represented groups.

## Information and Technology Transfer

MTI promotes the availability of completed research to professional organizations and journals and works to integrate the research findings into the graduate education program. In addition to publishing the studies, the Institute also sponsors symposia to disseminate research results to transportation professionals and encourages Research Associates to present their findings at conferences. *The World in Motion*, MTI’s quarterly newsletter, covers innovation in the Institute’s research and education programs. MTI’s extensive collection of transportation-related publications is integrated into San José State University’s world-class Martin Luther King, Jr. Library.

## DISCLAIMER

---

*The contents of this report reflect the views of the authors, who are responsible for the facts and accuracy of the information presented herein. This document is disseminated under the sponsorship of the U.S. Department of Transportation, University Transportation Centers Program and the California Department of Transportation, in the interest of information exchange. This report does not necessarily reflect the official views or policies of the U.S. government, State of California, or the Mineta Transportation Institute, who assume no liability for the contents or use thereof. This report does not constitute a standard specification, design standard, or regulation.*

**MTI REPORT S-08-01**

**The Fourth National Security Summit:  
Approaches to Passenger Screening**  
March 14, 2007

a publication of the  
**Mineta Transportation Institute**  
**College of Business**  
**San Jose State University**  
**San Jose, CA 95192-0219**

Created by Congress in 1991

## Technical Report Documentation Page

1. Report No. S-08-01	2. Government Accession No.	3. Recipients Catalog No.	
1. Title and Subtitle The Fourth National Security Summit: Approaches to Passenger Screening		5. Report Date March 14, 2007	
		6. Performing Organization Code	
7. Authors Symposium		8. Performing Organization Report No.	
9. Performing Organization Name and Address The Mineta Transportation Institute 210 North 4 <sup>th</sup> Street, 4 <sup>th</sup> Floor San Jose, CA 95112		10. Work Unit No.	
		11. Contract or Grant No.	
12. Sponsoring Agency Name and Address California Department of Transportation Sacramento CA 95819		13. Type of Report Symposium transcript	
		14. Sponsoring Agency Code	
15. Supplementary Notes			
16. Abstract  <p><i>The Fourth National Security Summit: Approaches to Passenger Screening</i> is the transcript of a symposium held on March 14, 2007. It was sponsored by the Mineta Transportation Institute and the American Public Transportation Association. For this symposium, numerous experts on security and terrorism, public policy makers, transit executives, and members of law enforcement were invited to participate in an open forum.</p> <p>Topics of discussion included: how public transportation is vulnerable to terrorist attack, and how public transportation has become a target for terrorist both in the United States and abroad; what techniques in screening can be considered the most realistic, reliable and effective; what new technologies may provide public transportation with increased security; how federal training programs and federal funds can most effectively be implemented and distributed nationwide; and finally, the best techniques in preventing terrorist attacks and mitigating risk.</p>			
17. Key Words:  Screening, Terrorist, Technology, Training, Random Screening, Selective Screening, Canine, Public Transit		18. Distribution Statement  No restrictions. This document is available to the public through The National Technical Information Service, Springfield, VA 22161	
19. Security Classification (of this report) Unclassified	Security Classification (of this page) Unclassified	21. No. of Pages	22. Price \$15.00

**Copyright © 2008 by the Mineta Transportation Institute**

All rights reserved

To order this publication, please contact the following:

Mineta Transportation Institute  
210 North 4<sup>th</sup> Street, 4<sup>th</sup> Floor  
San Jose, CA 95112  
Tel (408) 924-7560  
Fax (408) 924-7565  
Email: [iistps@iistps.cob.sjsu.edu](mailto:iistps@iistps.cob.sjsu.edu)  
<http://transweb.sjsu.edu>

## ACKNOWLEDGEMENTS

The Mineta Transportation Institute would like to thank the following individuals for their assistance in organizing and participating in the Fourth National Security Summit: Passenger Screening on March 14, 2007. (Listed in alphabetical order, except for Secretaries Mineta and Chertoff.)

- Michael Chertoff, Secretary, Homeland Security
- Norman Y. Mineta, Secretary of Transportation (ret.), Vice Chairman, Hill & Knowlton; Founder, Mineta Transportation Institute
- Bruce Butterworth, Consultant, Mineta Transportation Institute
- Douglas DeLeaver, Chief of Police, Maryland Transit Administration
- Rod Diridon, Executive Director, Mineta Transportation Institute
- Mort Downey, President of PB Consult; Member of Mineta Transportation Institute Board of Trustees
- Ron Frazier, Director, Office of Public Safety of Newcastle County; former Chief of Police, Amtrak
- Polly Hanson, Chief of Police, Washington Metropolitan Area Transit Authority
- Greg Hull, Director of Security, APTA
- Robert Jamison, Deputy Administrator, Transportation Security Administration
- Brian Jenkins, Director, National Transportation Security Center at the Mineta Transportation Institute
- Bill Millar, President, American Public Transportation Association (APTA)

The event was sponsored by San Jose State University (SJSU), the Mineta Transportation Institute (MTI), and the American Public Transportation Association (APTA).

MTI also thanks several other people for their dedication in producing this event and publishing the document: Communications Director Leslee Hamilton; Special Projects Director Donna Maurillo; Transcriber Meg Dastrup; Editor Frances Cherman; Technical Assistant Sahil Rahimi; and Webmaster Israr Qumer.

## TABLE OF CONTENTS

FOREWARD .....	5
EXECUTIVE SUMMARY .....	6
WELCOME AND INTRODUCTIONS.....	7
PRESENTATIONS	
BRIAN MICHAEL JENKINS.....	10
BRUCE BUTTERWORTH .....	17
DOUG DELEAVER.....	30
RON FRAZIER .....	36
ROBERT JAMISON.....	41
POLLY HANSON .....	48
MICHAEL CHERTOFF .....	50
QUESTIONS AND ANSWERS SESSION.....	56
CONCLUDING REMARKS .....	73

## **FOREWARD**

The recent attacks perpetrated against public transportation in England and Spain, as well as the continuing threat of a terrorist attack on American soil from both foreign and domestic terrorists, makes transportation security a pressing priority. Public transportation and transit have proven to be high-profile targets for terrorist attacks. Therefore, they deserve special attention and funds to help protect them.

While it may be impossible to completely prevent a terrorist attack in America, terrorist attacks can be discouraged and the damage they cause can be minimized through careful research, open discussion of policy, and proper application of security and safety funds.

The "*Fourth National Security Summit: Passenger Screening*" symposium addressed this growing concern, offered possible solutions, and became a call to action.

Numerous leaders, researchers and innovators were invited to participate in the open forum and to share their research and experience regarding finance, taxes, and public opinion.

New, innovative and realistic safety and security solutions must be implemented and financed so transportation and transit agencies and institutes across the United States can continue to be safe and efficient -- and can avoid attacks like those perpetrated in Spain and England.

Rod Diridon

Executive Director

Mineta Transportation Institute

## EXECUTIVE SUMMARY

The Norman Y. Mineta Transportation Institute (MTI) has been fortunate to receive funding, through the U.S. Department of Transportation's Research and Innovative Technology Administration (RITA) and the California Department of Transportation (Caltrans), to conduct policy-related activities in the areas of research, education, and information-sharing to benefit the United States surface transportation industry.

This document, *Fourth National Security Summit: Passenger Screening*, is the transcript of a symposium that was held March 14, 2007. It was sponsored by the Mineta Transportation Institute and co-sponsored by the American Public Transportation Association (APTA). For this symposium, numerous policy makers, security and safety consultants, police officers, transit executives, and transportation policy experts were invited to participate in an open forum.

Topics of discussion included the threat of domestic and foreign terrorist attacks on American soil, lessons that can be learned from the attacks perpetrated against public transportation in Spain and England, sharing successful screening techniques and other security measures, and the legal and financial ramifications of different screening tactics. With sources of funds dwindling – either through inflation or through a lack of financing – public transportation, aviation and transit-related infrastructure must anticipate new ways to discover stable, reliable funds for security and safety. As the threat of a terrorist attack continues, the most successful and cost-effective security and safety measures must be taken to save lives and preserve public transportation as a pivotal cog in the American economy and way of life.

Highlights of each presentation included:

- Rod Diridon and Bill Millar introducing the first speakers and setting the stage for the discussion on threats and security techniques;
- Brian Jenkins beginning the day by defining the threat that faces public transportation both in the United States and abroad;
- Bruce Butterworth discussing which techniques and technologies appear promising and which may be dead-ends;
- Douglas DeLeaver reporting what security practices have proven to be the most successful for the Maryland Transit Administration;
- Ron Frazier on the legality of certain passenger screening techniques and practices;
- Robert Jamison discussing how the TSA assesses risk and assigns funds for security and training;
- Polly Hanson summarizing the speakers' points;
- Secretary Michael Chertoff discussing the grant and fund application process at the Department of Homeland Security;
- A question-and-answer session in which the panelists, audience and speakers asked Secretary Chertoff about the Department of Homeland Security;
- A second, more in-depth question-and-answer session in which the panelists and speakers responded to audience questions.

**NORMAN Y. MINETA TRANSPORTATION POLICY SERIES**

**APPROACHES TO PASSENGER SCREENING**

**THE FOURTH NATIONAL SECURITY SUMMIT**

**MARCH 14, 2007**

**8:30 A.M. TO 3:00 P.M.**

**ROD DIRIDON:**

Good morning, my name is Rod Diridon, and I think I've met many of you. I'm the Executive Director of the Mineta Transportation Institute and the past president of APTA, the American Public Transportation Association. It's nice to be here again at a program which is jointly sponsored by the American Public Transportation Association. Before we start, I just have a quick commercial, and I assure you this is the only commercial you'll get. The Mineta Transportation Institute is now in its second decade; we were founded in 1991 by ISTEA (Intermodal Surface Transportation Efficiency Act), re-authorized in 1998 by ISTEA number 2, and re-authorized again in 2005 by SAFETEA-LU (Safe Accountable Flexible Efficient Transportation Equity Act: A Legacy for Users). We have won national competitions to sustain our position as one of the ten tier-one centers of excellence in the University Transportation Center's program, both in 2002 and again in 2006. We are very pleased to be able to continue to serve the nation as a transportation policy research center.

Our actual name is the Norman Y. Mineta International Institute for Surface Transportation Policy Studies, and that gives me job security because I think I'm the only one that can say the name. We now have 157 certified PhD-level research associates working with the Mineta Institute, all around the United States and in many foreign countries. We concentrate on counter-terrorism and security research, in terms of the threat side of the issue as well as the response side, although we're going to concentrate on the threat side today. We also concentrate in transportation finance, research, as well as transportation land use policy activities, especially as it relates to smart growth and station-adjacent densification, transitory development activities. We have published just under a hundred recent projects since we began. Each one of those is a peer-reviewed research report, and many of them have gone into symposia and peer-reviewed journal articles. We also have a Master of Science Transportation Management through the CSU

(California State University) system that we teach; this program has a California Department of Transportation videoconference bridge from 24 sites around the state of California and the western United States. So that's the commercial, and if you have bright young people, I encourage you to send them to our Master's program. We have at least one Master's student here in the room with you today from our Master of Science in Transportation Management.

Before we begin, I would like to thank Bill Millar of the APTA and Greg Hull for assisting us in presenting the summit today. This is our fourth National Transportation Security Summit, with the first occurring back in 1996, believe it or not. So we were way ahead of the curve back then, partly because we captured Brian Jenkins as he was retiring from Loran Corporation and going off to help found the Crowell International Security Corporation, so we began this investigation into National Security back before it was fashionable to do so.

The American Association of State Highway and Transportation Officials is a co-sponsor of today's event, and we appreciate that. We are taping the proceedings, and we will publish the proceedings. So when we get to the Q&A portion, if you would say your name before you ask your question, then we will be able to identify the person who asked the question. This is all part of the research process, because you not only will learn from the proceedings, but you will be helping us teach others about today's topic. It is now my pleasure to introduce the person who will act as the MC for the first part of the proceedings, Bill Millar. Bill is the president of APTA, and he became president back in 1996. Bill has been the longest-serving president of any of the major national transportation organizations. A ten-year seniority in this tough kind of a job is remarkable. Bill was also the general manager of the Pittsburg Area Transportation Association and the Allegheny County Transportation Authority, he was the president and founder of the Transit Cooperative Research Program with TRB (Transportation Research Board) and he has had many honors throughout his illustrious career. And now, Bill Millar.

**BILL MILLAR:**

Good morning all, and Rod, thank you very much for that kind introduction. We at APTA all very much enjoy working with the Mineta Institute. Let me say it's too bad that we have to have the fourth security conference relating to public transit. I think all of you will agree, if we could end these because there was no threat of terrorism, we'd all be a lot happier. But that is not the case, and our public transit industry continues to struggle with how to make our customers, our

employees, and our communities safer and more secure. We have learned many, many things over the years, and we have shared a great deal of information with each other. Today's seminar is a continuation of that series.

I don't know whether you noticed or not, but when you came in the hotel and you came down the elevator or the escalators and you walked towards the salon, there is a big sign out there. It says "Protecting Our Nation, Protecting Our Future." Now, that sign actually was put up a couple days ago because the C17 supplier industry fly-in, and so it was about a specific piece of military hardware, but it seems to me that that sign is the perfect theme for this conference: "Protecting Our Nation, Protecting Our Future." Earlier this week, you may have heard that I had the privilege of announcing that our public transit agencies had served over ten billion customers last year. Ten billion. That's a big number. That's more than all Americans who attended football games, major-league baseball games, National Hockey League games, NASCAR, or who ate a hamburger at McDonald's, Burger King, or Wendy's. That's a hell of a lot of people. And that's the dimension of the problem that we have. So we have a great responsibility, to our customers, to our employees, to our nation and our communities. And I hope at the end of today, we'll know just a little bit more. Now, let me introduce our presenters today, and while for most of us in this audience, these gentlemen, as they say, need no introduction you're not allowed to not give an introduction, so we've got to give them their due.

First, Brian Michael Jenkins, Director of the National Transportation Security Center at the Mineta Institute for Strategic Transportation. Brian is one of the world's leading authorities on terrorism and counter-terrorism. He's been a counter-terrorism research team leader and a research associate with the Mineta Institute since 1996. In that same year, President Clinton appointed him to the White House Commission on Aviation Safety and Security. Mr. Jenkins is also a Senior Advisor to the President of the Rand Corporation, and he is a counterterrorism advisor to New York City Police Commissioner Ray Kelley. Brian was a captain in the Green Berets, serving with the Army Special Forces in the Dominican Republic and Vietnam. He later returned to Vietnam on special assignments as a civilian. He has a BA in Fine Arts and a MA in History from the University of California at Los Angeles, has pursued studies in Mexico, Guatemala, is a Fulbright Scholar, and received a second fellowship from the OAS (Organization of American States). He's also the co-author of many MTI reports, and they're listed in the back of your program today.

With Brian is Bruce Butterworth. Bruce is a consultant at the Mineta Institute and has had a distinguished government career working in Congressional, senior policy and operational levels since 1975. He was a staff member for the House Government Operations Committee, where he ran investigations and hearings into many transportation safety issues, particularly in the area of security. He ran the FAA's (Federal Aviation Administration) command center, and successfully managed the resolution of hijackings and security emergencies. As Director of Operations at the FAA, he was responsible for 900 field agents and oversaw the conversion of the original Air Marshal Program into a full-time program with very high standards. Mr. Butterworth was also part of the response team to the Pan Am flight 103 attack and was a key player in the ValuJet and TWA crash investigations. As an Associate Director of the U.S. Holocaust Memorial Museum, his responsibilities have also included security for that museum. Mr. Butterworth has designed and implemented a best-practice procedure for dealing with mail that is possibly contaminated with anthrax powder. In addition, he has co-authored the Mineta Institute analysis on passenger screening and public transit, and co-authored a study of passenger air cargo security for the Center for American Progress. He holds a Master of Science degree from the London School of Economics and a Bachelor of Arts Degree *Magna Cum Laude* from the University of the Pacific, where he was a California State Scholar and a Rotary Foundation Fellow. We couldn't have two better-qualified folks to talk to us on these topics. And with that, let me introduce Brian Jenkins.

**BRIAN MICHAEL JENKINS:**

Thank you very much, Bill. A few weeks ago I testified before the House Appropriations Committee and last week before the State Senate Transportation Committee in the State of California on a similar topic. Basically we're trying to deal with the dilemma that we mention in the opening page of this report, a report that we want to talk to you about this morning on the selected screening of rail passengers, and how it all comes down to allocating resources. That's what really counterterrorism and security are all about. It's not about Jack Bauer and car chases. It really comes down to allocating resources. Modern security looks more like a construction project than a car chase. We face a dilemma because we know that the terrorist threat is real and the terrorist threat to surface transportation is real. Fortunately, it's statistically remote. We know that transportation targets are attractive to terrorists, but there hasn't been a successful terrorist attack on surface transportation in the United States in the last ten years.

When I was part of the White House Commission on Safety and Security in 1996, we were making a pitch to Congress for the huge sum of \$260 million to be devoted to improving aviation security and safety in the U.S. We wanted \$260 million, plus a commitment from Congress for an additional \$100 million each year for the next five years. If you think of those numbers, then compare them to what we're spending now on homeland security: those figures are minuscule. And yet I was asked the question and challenged by one of the Congressmen at the testimony. He said, "Mr. Jenkins, when was the last hijacking in this country? Why should we be spending the taxpayers' money to deal with this issue?"

We know that plots have occurred, in terms of terrorists looking at surface transportation targets. Fortunately these have been thwarted. But if, heaven forbid, something were to occur tomorrow in this country, we would all be shocked. However, none of us could reasonably claim that we were surprised by such an event. In preparing for this, I went back and re-read some of the things that we had said at the security summit that took place at the request of then-Secretary Mineta on October 30, 2001. This was 49 days after 9/11, and the Secretary had asked Rod if we could quickly pull together some guidance that we could give to the transportation operators that would help them address the security challenge in the immediate wake of 9/11.

Looking at my comments at that time, I had said I thought that there were two al-Qaeda plans on 9/11, or preceding 9/11. One was for the actual 9/11 attack itself and the second plan was a business continuity plan for al-Qaeda for the survival of their leadership and for their continued communications between that leadership and their operatives and constituents worldwide. They planned to continue operations once the leadership went underground. In October 2001, I'm saying this thing isn't over, that these guys have got another plan, they're going to hide out, they've got a business continuity plan here, they're going to continue to communicate, continue to recruit, continue to radicalize and continue to be in business. And unfortunately, that has proven to be the case. The other thing that's striking is, if you go back and read the October 2001 report, how far we have come in terms of our organization, our allocation resources, and our sophistication in dealing with these security issues. I mean, this was pre-Department of Homeland Security. This was pre-TSA, this was pre-allocation of the billions of dollars that have now been spent on domestic security. Unfortunately, it was also a long time ago in terms of the threat. It was pre-Madrid, it was pre-London, it was pre-Moscow, it was pre-Mumbai and all the other attacks that we have seen take place since then.

We were able to pull together that conference in October of 2001 only because, as Rod indicated, the research had already begun in 1996. Had we started the research on 9/11, we sure as hell wouldn't have results 49 days after 9/11. We were able to draw on that. And indeed that research came about as a consequence of foresight by the Institute and foresight by some officials in our government. I remember that when we were conducting our meetings with the White House Commission in 1996 and 1997, in the background of our discussions on aviation security we had the Tokyo incident involving sarin nerve gas in 1995, and the bombing campaign against Paris subways in 1995 and 1996. So, while the issue then was commercial aviation, all of these were attacks on surface transportation.

We have a hell of a problem, in terms of surface transportation, reconciling the solutions that we are attempting to apply for commercial aviation, such as 100 percent screening. That simply isn't going to work for the billions of passengers that you deal with in surface transportation. It was when I was a member of that commission that I first met Bruce and we began to work on these issues in 1995, primarily looking at passenger screening in the context of aviation passenger screening, but also trying to tackle the current topic. Thus, Bruce was the natural person to turn to again.

We have made undeniable progress against terrorists since 9/11. I think future military historians looking at this campaign will say that perhaps the most important achievement was the dispersal of the training facilities in Afghanistan, not simply because of the training they provided. You don't need elaborate camps in Afghanistan to provide training. But the camps in Afghanistan were in easily accessible destination points for Jihadist volunteers from around the world. These camps allowed them to come together and create networks of relationships that they still rely upon to carry out operations worldwide despite our disruption of their command and control systems. The other thing these camps did was to provide a continuing flow of talent for al-Qaeda's operational planners, which allowed al-Qaeda to operate at a much higher level than any previous terrorist organization that we had seen. I like to tell people it's the same reason why basketball in the NBA is better than basketball on a high school team. A high school team can recruit from a local neighborhood, a university team can recruit from the nation, the NBA recruits from the entire planet. Once you're recruiting from a reservoir that size, you can find a lot of guys who are 7 feet 14 inches, who can make 3-point shots. And it's that skill level that they were able to put together, and that's what made those camps important.

By destroying these camps, we have removed some of the key operational planners, and that represents a real loss of talent for al-Qaeda. We kept the top leadership on the run and, as a consequence of the unprecedented focus and cooperation among law enforcement and intelligence agencies, we've been able to make the environment a lot more hostile towards them. So the kinds of things they were able to do in the planning of 9/11, such as have people go back and forth across borders, send large sums of money abroad, have communications that could be intercepted – all of those transactions have become more dangerous for them now. But we haven't dented their determination one bit. They continue to come at us, they continue to communicate, they continue to radicalize, they continue to recruit, plan and prepare operations.

I think this has been a major failure of our strategy. You must think of the Jihadist threat as a complete cycle that begins not with the terrorist operation but with radicalization and recruitment of angry young men and turning them into dangerous terrorist weapons; then moving that up through the discussion, planning, and preparation of operations that lead either to victory, death or capture. Our actions were understandable immediately after 9/11, but it's unfortunate that we have continued to focus exclusively on pounding that operational portion of it, which just breaks the surface. We really haven't had a front-end strategy that deals with the continuing radicalization process. This condemns our strategy to being the equivalent of stepping on cockroaches one at a time. Unless we can really impede that front end, we're going to be dealing with this thing forever. Indeed, in terms of demonstrating capability, they're operating at a higher pace today than before 9/11. We now see an escalation of the insurgency in Afghanistan, and continued fighting in Iraq. These locations have become the training academy for the next generation of terrorists that we're going to be dealing with for the next ten or 15 years. And the skills being acquired in Iraq are much more fungible than the skills that were acquired in Afghanistan. Afghanistan is a moonscape, while 70 percent of Iraq is urban. Learning in a terrorist organization is a function of frequency of operations. When a terrorist group carries out several attacks a year, they've got several opportunities to learn. In Iraq, we're looking at a couple of hundred attacks a day. Now that's a lot of opportunity for learning, for innovation. And those skills spread through the Internet and through the dispersal of veterans themselves. What we are seeing today in Baghdad is what we're going to be dealing with five to ten years down the road worldwide. Currently we have a similar high pace of terrorist activity. In the last six to seven months, we're seeing more than 30 large-scale terrorist attacks around the world, not

counting anything in Iraq, or Afghanistan, or Chechnya. These have been in Bali, Istanbul, Madrid, and London. That's about one major operation every sixty days. Now, if we add that to the more than 30 plots that were thwarted, although it's hard to count things that don't occur, it becomes closer to one every thirty days. So, we have a batting average of about .500, in terms of being successful. So there is definitely a continuing threat, mostly bombings, mostly—but not all—suicide attacks. But don't become mesmerized by this suicide issue because the worst incidents in Mumbai and in Madrid were not carried out by suicide bombers. So, when people talk about security measures and they say “Well, what kind of security measures can deter suicide bombers?” , as Bruce will explain in a moment, if we could set the bar so that we push them all to become suicide bombers, that in itself is a hell of an achievement.

Ten bombs went off in Madrid and killed nearly 200 people. Lots of people who were involved in that operation are on trial right now. In fact, Spain is on alert because of the potential for terrorist attacks during those trials. In London, four suicide attackers killed 52 people, apart from themselves. It sounds callous to say so, but 52 people dead is better than 200 people dead, and that's the way we have to look at this, as a numbers game.

So let's go over some of the trends in their overall organization, which is much more decentralized now. Operations have a higher local content, which means that there are far fewer transactions for national intelligence services to pick up. So, we can't be waiting for intelligence to tell us that they're coming, because while national intelligence services are watching for communications, movements of people and money, there are simply far fewer international networks than there were before. This places a great deal of pressure on local law enforcement to understand what's going on in their communities. This is something we have to work on in our nation. The Jihadists understand this and discuss it openly. Before 9/11, there were about four or five Jihadist Web sites. Today there are thousands of Jihadist Web sites, which is a reflection of radicalization. These Jihadists see the attacks in Madrid and London as great successes. I mention Madrid being on alert right now because of the trials going on. France is also on very, very high alert. I was talking about this the other day and there were some French officials present and they said that because France has presidential elections coming up in May, they are very concerned that Jihadists who are very active in France will use that as an occasion to try to replicate the Madrid attacks.

The Jihadists talk about targets that have emotional value, iconic value, landmarks, things of that nature. But they also talk about body count, and it appears that the desire for body count may be the true driving factor for them. They basically want to kill a lot of people. That's the way they demonstrate their prowess as warriors. And therefore, that pushes them in the direction of softer targets and more reliable tactics. Unfortunately, in that regard, surface transportation becomes a very attractive target to them.

We know it's in their playbook. We know that even in this country we had a plot in 2003 to release cyanide on New York subways. We had a plot in August 2004 to bomb the Herald Square subway station in New York. Both of which were thwarted by intelligence. There was a plot in 2005 to spread ricin on the Heathrow Express, the train between London and Heathrow Airport. In July 2005 there was another failed attack on the London subways in addition to the one that occurred early in August 2005—a plot to release gas on the subways

There were plots in Australia, Milan, the Philippines, and again in New York. Bombs were discovered aboard trains in Germany which fortunately didn't go off. Why is there an attraction there? It's just purely callous in operational terms. Think of yourselves for a moment as terrorist planners. You're going to make an investment of time and money, you're going to take risks, you're going to try to kill a bunch of people, and you're going to put down a bomb. What kind of return can we expect on that investment? If we look at these episodes, just these recent episodes that have occurred, we see that they're getting a return on investment of about 24 fatalities per bomb. The way they run that up further, then, is you go for multiple bombings. One bomb equals 24 dead, okay, ten bombs, we get 240. Some of them don't go off, so you end up between 190 and 200, but that's the way this works. They also create a great deal of alarm, disruption and economic harm, all of which is basically immeasurable. This is attractive to them because, operationally, it's easy. This is public transportation; it is conveniently accessible to the public. To protect ourselves, it's not a matter of creating moats or elaborate security measures. We will destroy public transportation if we do that. Moreover, surface transportation contains crowds of people in contained environments, and that enhances the effects of explosives and unconventional weapons. Of the four bombs in London that went off – one in the bus, two in shallow tubes – the one in Kings Cross, which is a deep tube in London, had very little tolerance between the side of the carriage and the tunnel itself. And what does that mean in terms of the explosion? It had nowhere to go except up and down through the carriages, and that created

massive casualties. From the chronology and analysis that we've done at Mineta Institute, we can take a look at this more broadly and see that two-thirds of the attacks on public transportation were intended to kill a much higher percentage than terrorists' events against all other targets—that 37 percent of ground transit attacks resulted in fatalities compared with a 20 to 25 percent average, overall. More interestingly, 75 percent of the fatal attacks involve multiple fatalities, and 28 percent involve ten or more fatalities. So again, public transportation is a “killing field” for them.

When we look at the targets they talk about blowing up bridges, like bringing down the Brooklyn Bridge. These big infrastructure things are tougher to take on, nearly impossible, so they're going after the people. About half of these attacks involve attacks on buses of various types, half of them involve attacks on rail, and only about 5 percent go after infrastructure.

We've talked about Europe, but it can certainly happen here. There was the plot in 1997, the so-called Flatbush plot. Police discovered that purely by good fortune. One of the conspirators got cold feet and went to a couple of cops, and in barely comprehensible English, tried to explain to them that something was going to happen. And instead of just blowing him off as a nut, they took him seriously, went to the bureau, and mounted an operation. And sure enough, there was a group of terrorists with suicide belts, prepared to carry out bombings in New York subways.

An attack on U.S. soil would certainly not come as a surprise. We couldn't claim that it was a surprise, but we face some real constraints. We're not going to be able to screen ten billion people. There are fewer than two million people a day that board airlines in this country. We have many times that number use surface transportation in this country, with thousands more points of access. We have about 430 commercial airports in this country. There are more than 430 stations on the New York Transit System alone, so we know that isn't going to work there.

There is also an inability to bear higher costs. We have put the aviation security budget into the federal budget, and we spend billions on that. I think the amount being spent in the federal budget or being allocated for the 2008 federal budget for all surface transportation security is about \$175 million. Local governments are strapped, so we simply aren't going to have the resources for this. We know we're also going to face legal challenges to these issues, and in some cases, public resistance.

That brings us back really just to what we talked about at the beginning—the efforts at Mineta Institute to explore how we can address these issues. And there’s a philosophy behind the Mineta Institute’s approach here, which is we know that a commercial aviation security model isn’t going to work, for all sorts of reasons, and it is inappropriate to take a federal regulatory approach to solve the security issue. Our surface transportation communication system is too varied, too complex. It is a function of local operators, local governments, and I do not see the utility in attempting to impose a federal regulatory rigid rule-based posture, which is the way aviation security is run.

The best approach is to look at lessons learned, look at the cases, so that we can understand what has happened, identify the best practices, and provide that information to those responsible for security in these local systems. Then we need to let local regulators use common sense to determine what is applicable to their particular systems. It’s not going to be the same solution in Duluth as it is in the District of Columbia, nor should it be. So in order to have a best practices approach, we need to have case studies that are regularly published. That’s why we maintain the chronology, so that we can provide the information. It’s not to tell you what to do, but to demonstrate the lessons learned from these episodes. Then the local authorities figure out how to take these studies and configure them to their systems.

Well, that’s really my segue for the research that is going to be presented this morning about selected screening. So with that, I’ll turn it over to Bruce.

**BRUCE BUTTERWORTH:**

Thank you very much, Brian. Before I start, I do want to thank a couple of people in the audience for their help in this research: Stefan Parker from the TRB (Transportation Research Board), and Greg Hull from APTA (American Public Transportation Association). Also, a quick reference to a small thing on my own bio; the piece with the Center for American Progress has not yet been published. My co-author, is P.J. Crowley, who has also done some work in mass transit.

So here’s the question we need to ask ourselves: We know that this is a high value target, so what do we do? There’s been silence about screening, and we both decided to try to break that silence. I know that the upcoming work by the Transportation Research Board, which you will hear later, is a very fine piece, and is going to help that along. But we wanted to put this marker down, and suggest a way forward. We wanted to explore screening, particularly selected

screening, as a viable security option in mass transit. We started considering 100 percent screening, and, as Brian mentioned, we don't think that's possible. Then we asked, "Do selective screening methods make sense?" If they do, then how do you select those passengers when there's no specific intelligence? Now, those of us who have worked in this area know that 90 percent of the time, there is no specific, credible, immediate intelligence. You're dealing with vague situations, so you have to start looking at selective methods: combinations of selective methods for a variety of scenarios. We just took the variables of specificity, credibility and longevity and tried to put them in a sensible way to give operators a chance to start with combinations that might work best.

Since technology is prominent in the American psyche, there has been an awful lot of emphasis on technology. My own opinion is that there is a tendency to put too much focus on what it can do, and that we are unrealistic about what it takes to make it work. So we wanted to look at what technology can do for the two functions of screening, which are selection and search. And then we believe that you have to have a good security program, and that means good quality control, good management.

Now we took the courageous step by saying what we all know, which is that stopping every attack is not possible. It may be a good campaign sound bite in an election year, but it is not possible, in general, certainly not in an open system like public transit. What is possible and realistic is that we can reduce risk.

So how does a selective screen system actually help do that? As Brian mentioned, most of the devastating attacks are done by people who seek to escape, which means that all of the methods you have that pierce the anonymity of the attacker, CCTV and others, have some value. The people want to escape without punishment, to fight another day, so to speak, and there are an awful lot of methods that are currently out there to accomplish this goal.

As you reduce the pool of people who want to escape, you then have the operatives focused on suicides. But the commitment and resources required to develop a suicide attacker are much higher. We know this from studies. Suicide is not a natural act. It takes a great deal of commitment, and it takes great deal of control from the operatives. Probably the best example we can find is that in two months in Madrid, 13 conspirators collected together, bought dynamite, and managed to create ten bombs which caused 191 casualties, and if all of the bombs planted in

the station had gone off on time, that structure would probably have collapsed, and the number of casualties would have been much higher. Meanwhile, it took six months for four attackers to carry out four suicide attacks in London. Now granted, these were only data points, but it does tend to show that it is harder to find suicide attackers than it is non-suicide attackers, while the rate of casualties-per-bomber is about the same. The other thing is that even suicide attackers are on an operational mission, and they're trying to achieve an objective. If they see that they can't achieve that objective, they will probably turn around and go back and try something else.

So what does partial screening do? Well, it can certainly complicate planning and increase the chances of interception. Now, as Brian mentioned, an awful lot of the groups we're most worried about are the homegrown groups, not the ones with centralized direction. Homegrown groups can stop, go back, re-plan, readjust, re-communicate, acquire different techniques, and acquire different detonators. But all of this increases the chances that they're going to bump into someone or something that can trigger a law enforcement response.

Secondly, there are cases where people walk up and decide it's not worth it. There is actually a classified example that comes from 1995; this happened on an airplane that was leaving Asia. We also know that there are instances in which the perception of what security can find made the attacker use a different method, which resulted in an ineffective conspiracy. In this case, it was Ramsey Usaf, who changed his tactics to using liquid explosives and different bomb components, which caused a fire in the Manila apartment building, which ended up bringing that plot to the attention of the authorities.

Of course, the final factor is that selective screening can cause the attacks to be diverted to locations where fewer casualties are caused. Now, we don't say this in public, although we used to say this in aviation, but if attacks are diverted to other lower-value targets outside of mass transit, it may not be all that great for the nation, but it certainly is good for mass transit. It reminds me of the story of the two men running away from a grizzly bear, when one man turns to the other and says, "Why are we running? The grizzly bear can outrun us." And the fellow says, "I'm not trying to outrun the grizzly bear. I just have to outrun you."

Deterrence is not paper tanks. You just don't put it out there, you don't be Pan Am and get some dogs from the local kennel and run them in front of your airplanes, and pretend that everything is just fine. Because people watch what you're doing and they will know if you have a system that

can or cannot actually detect something. So deterrence depends on good detection, and good detection depends on well-run programs. You can also increase deterrence, and in the surveys I'm going to mention in a second, we found a lot of excellent ways to increase the deterrence.

- You can adjust the screening method;
- You can change your screening locations;
- You can interject police randomly and sometime massively into stations; and
- You can increase interaction with passengers through what amounts to community policing.

My wife used to be in a social club in the 50s, which was called KEGs: Keep 'Em Guessing. And I think that's probably the best summary of this. Passenger screening does reduce risks and is a viable security option for elevated threats. It creates deterrence; it has the possibility of detection. Properly planned, it can be implemented rapidly; it can be re-deployed in changing patterns, up and down. It increases the alertness of staff, and it's going to help in detection of other crimes, such as theft, assault, the kinds of things that when you talk to the transit security chiefs, are much more imminent and commonplace. And the tag line here is that some is better than none, and lots are better than some.

So, now we can review some of the selective screening methods we reviewed. We went through a number of selection methods, starting at 100 percent against. This is a rather bold statement, but not only do we think it's impractical, we think it's dangerous. There are two reasons. One: peak hour at Penn Station, with all the trains going in all directions during the rush hour, equals 60 hours at O'Hare. That's a phenomenal one hour. And what's even more impressive is that one peak hour at Lexington Avenue in the rush hour direction on two lines equals about 7.2 hours at O'Hare, or roughly a third of the time at O'Hare during the entire day. If you cannot create the staffing and the methodology to handle those crowds, guess what happens: you create further crowding and greater lines, and you create them at a closer distance to the bad guys, and what you've just done is the unforgivable: you've made the system easier to attack. So that's why we say that not only is it impractical, it's also dangerous.

A hundred percent screening would essentially take the "rapid" out of mass transit. So, next, we decided to look at random screening, which is simple enough. It's a mathematical formula

independent of other factors, including what the screener wants to do. It can be one in every 20 passengers, or a handheld calculator that basically assigns a number between one and forty randomly, and everyone who has a number between one and four ends up being selected, which results in a 10 percent selection rate. A key to random selection is that it should be very hard to predict by observation. Someone watching this should not be able to predict what's about to happen.

Then we look at selected methods, which use ways of looking for indicators of an attack. Logically, we look for an emphasis on an appearance and behavior. The National Transportation Institute FTA (Federal Transit Administration) funded training for transit employees. It looks at attitudes such as hesitancy; body language, such as sort of a trance-like stare and red neck; rigidity, profuse sweating; and other things that are pretty hard to control unless you're really a professional. In addition, strange behavior in crowds, hand signals, and other things of that sort. There are an awful lot of good things that trained officers, undercover or uniformed or staff, can find. They can look for clothing in bags, if it's bulky in the summer, or bags that are large enough to carry a ten- or 20-pound bomb.

On tickets and IDs, I have some good news and some bad news from the world of aviation. We know that it is hard to create a pre-passenger selection. I can't tell you how much money and pilot programs have been wasted trying to do this. I don't think that's going to happen in mass transit because you're always going to have a population that will pay cash for tokens because of the economic characteristic of who uses mass transit. So, I don't see passenger pre-screening as any kind of a viable option in the future.

We also have time and route of travel, which can tell you who's going to be close to targets of symbolic importance. Technology isn't yet ready to do selection. Canines have some possibility for teams that are trained on arriving passengers, although not on bags. In addition, there is the very sensitive question of racial profiling, which involves racial profiling for specific ethnicity, national origin, age, and/or gender.

If racial profiling is not linked to intelligent choice, it's illegal, and it's dangerous because we know that terrorists have evaded profiles, both by dressing around them, or by using people who don't fit that profile. It is not beyond the realm of possibility to find a white female Jihadist convert in the U.S. who could carry out an attack, for example. Now by contrast, if you had a

piece of intelligence that said we've got suspects who are 25-year-old males from Southwest Asia, it would be stupid to spend an awful lot of time looking at 70-year-old black or Asian grandmothers.

There are a variety of search criteria and methods, which can usually be conducted using common sense. An examination would include clothing, carried articles, bags or packages, and ID, if we ever get to that point. An examination can be conducted by visual check, hand-search, trace detection, which looks for the particles either on the surface or in the air, or bulk detection, which looks for the mass and atomic composition of the explosive itself. Canines are really four-legged trace detectors that follow a trace to source, but unfortunately they don't have the ability to tell you when they're operating and when they're not.

Brian has mentioned the issue of limited resources, and I must stress that even selective screening is a labor-intensive effort where costs can become a real problem. Transit agencies operate on the basis of public subsidy or public support, both for capital and operating expenses. When I asked many different public transportation agencies about how long they could sustain a selective screening effort using current staffing and police officers, the answer was generally about two to four weeks, and then help would be needed.

Legally, although this is actually contracted a bit with the high court, selective screening seems plausible. The U.S. Court of Appeals in New York ruled against the ACLU's attack on the New York subway systems' screening. And everyone I spoke to said, with that decision, they were much more comfortable putting a screening system into place in New York, such as one similar to that found in New Jersey, and that they believed it would survive legal scrutiny.

If we were to implement selective screening, how would the public react? I always remember Barney Frank when he was defending Congress saying, "The public ain't no great bargain either." And although we serve the public, we have to understand that they want many things, and that you'll hear from them if they don't get it. The public wants screening to be passive and not intensive, and they don't want it to be intrusive. I remember trialing this at airports back in the 1990s and finding out that even if a machine only shows a stick figure on the screen, they consider it an invasion of privacy. In addition, the public wants it to be egalitarian, so everybody gets screened in the U.S. There are flight crews that have to go through screening checkpoints

when they could easily go behind to an access door to get onto the airplane. If we didn't screen them, there was going to be a problem in terms of managing the screening checkpoint.

We know from a Harvard study that we quoted in the report that the tolerance for inconvenience goes up only when the promise of safety is absolute. When someone says there is no risk of anything bad happening to you, then the public will start to tolerate things. If someone doesn't say that, then objections tend to be brought up, and those objections tend to go up where selective screening is concerned, primarily with minority populations who have a very good reason to suspect government practices. One has to be aware of that, and since transit is used by different demographics in the population, it's always going to be a factor. Also, we know that the public withdraws support as time goes by without an attack or a publicized threat. Whoever is out there from TSA and DHS (Department of Homeland Security) knows this. A week after 9/11, you could have done just about anything, and everyone would have agreed with it. When no event happens over time, then the questions start to be asked: Why are you doing this?

While a long period of time has passed since the last major attack, the current terrorist threat may actually be the same or could even be greater. Professionally-run programs are your best defense, and a persistent campaign of public and passenger education. A solution to public displeasure with a screening process means that you need to have a place for the public to go to complain. It's best to stop a small campaign before it becomes a large one. Also, avoid promising something you can't deliver. If you say this makes the system 100 percent safe, you will always be criticized. Because the media will test it or the government will test it, and the results will be leaked to the media, and you will be found not being able to do what you promised.

We did some quick interviews with public transit folks, and here are some of the common threads we found in our survey, which I'd say is about 95 percent accurate. These were telephone interviews, which included some of the people in this room. Here's an aggregation of results. Everyone saw public transit as a possible or even likely target of terrorism. I think everyone saw that screening is going to be needed, but that a 100 percent screening is not possible. There were different emphases on limitations for resources, public reactions, and senior management anticipation of public reaction and legal liability. With the combinations depending on location. Generally, the farther you are from the East Coast, it seems, and the farther you are from the

WTC, the harder it is to implement a comprehensive screening process. Everybody wants better links with the intelligence agencies, and everyone wants workable solutions practically drafted.

When I was in aviation security, I can tell you for sure that nearly half of the times we revised security directives, it was because we didn't get the technical language right, or because we didn't have access to the people who could help us draft it properly. So getting this right in a way that is easily understandable for people in the transit industry is pivotal. There is an informal network, the COPS Committee of APTA, and many of the people I interviewed said they got some of their best information from COPS. Both private sector and government-funded best practices have developed and have been improved. The NTI training that I mentioned before is a commonly adopted method of screening. It involves the behavioral assessment security system which was first developed by Boston Logan, and then has been improved and is still being improved upon.

However, there have been some problems. There seem to be unrealistic expectations about what technology can provide to a non-line-based selection method, but everyone wanted more focused TSA investment in technologies. There were many people that said, "We'd like to have TSA act as a clearinghouse because we're often caught on the horns of competing vendor dilemmas about what they actually can deliver." Policy and planning, a lot of different variations, basically those that had screening programs now had everything written out; those that were far away from implementing them don't.

The ratio in resources for transit agencies differed widely, and everyone had methods to augment from outside sources. New Jersey had some of the most robust programs for training state troopers, and public transit agencies close to Washington tended to have more agreements with federal agencies. The use of undercover agents/officers varied: ones that have screening systems in place tended to place a high emphasis on them, and those without tended not to. All of the transit agencies employed very different deterrence; they had very creative methods of increasing deterrence. They did it through police surges, active community policing programs, by getting people out there to talk with the passengers. One agency had the janitors working to help in security because who knows better about what is right and what is wrong in the work environment than a janitor? And, of course, utilization of trained staff to get them out of the fare booths and get them interacting with passengers. All of these groups had very innovative training

techniques, very innovative public participation campaigns. However, no matter what, implementing new screening techniques can only be sustained for two to four weeks.

Quickly, I'll discuss the New York and New Jersey system. The screening is all-voluntary, the searching of bags is done with explosive trace detectors (an ETD), or by canines. Passengers are selected at random, but that random method is shifted, and the stations are often chosen without announcement. The officers at these stations, both uniformed and undercover, are trained in behavioral assessment security screening methods. The undercover officers add something to a screening process. The public may look at this, and say, "Well someone can just turn around and leave." Just remember that undercover officers are watching everyone that goes through and also documenting people who decide to evade screening. I think in a way it's creating an event to which you get a response which you then watch. There is one transit system that's experimenting in the use of canines to select people for the screening process, that's a promising program.

We did run into common threads here, which are that if there was an attack or a threat, there would be an implementation of screening. It would be a program similar to that of New York or New Jersey, with methods which used intelligence, random profiling and behavioral profiling, and the focus would be on stations with high volume and name recognition. But transit tended to ignore small station entrances and non-rush hour times.

The last thing I wanted to mention is that almost everybody feared the Friday afternoon, usually happens around two or three, where you get a piece of vague information, it's not clear what the bureau (FBI) wants you to do with it. But I think it's time for them to go home, and they drop it in your lap and say, "Here; it's yours." And now you have to figure out what to do with it. Everybody has expressed concern about getting a vague threat with no defined exit criteria.

I won't spend a great deal of time on technology, except I want to make two basic comments. One is that the threat mass is about ten to twenty times that of aviation, so that makes detection of an individual bag or an individual person much easier, and that should allow you to get a higher probability of detection with much less error. The difficulty, of course, is throughput. There are a couple of caveats in technology you have to define what you're looking for and what you're not going to look for. You have to decide that you're not going to look for knives. You have to decide that you're not going to be caring about explosives below a certain mass. That's a tough call to make, but you will end up having to make it. By the way, it's made in aviation

today. Technology only provides new data to an operator. That data can be confusing, or it can be clear, but it has to be evaluated. Your focus can't be so much on the technology, but on the operator who's using it. This means you can't underestimate costs or the management burden of this.

We came to this conclusion after consulting with the DHS, and we don't think that current or near-term technology is going to be capable of performing selection. It can, certainly, less intrusively and more effectively search those selected. We do think there's strategic investment needed in standoff technologies (technologies that can passively look at individuals or crowds at distances of ten meters or more). However, the challenge of developing standoff technologies is significant. But I think it can be surmounted, with a rough estimate of five years—and many more years for crowd—assuming the most optimistic scenarios of deployment and as long as we're focused only on explosives. If you add searching for biological, chemical or radiological weapons to the equation you're talking about a whole different set of problems.

When we took a look at this, at the selective screening methods and the random methods, we ranked them. We think random should be the official method. It helps pass legal muster, and it certainly can be managed to introduce uncertainty for the attacker. Behavioral profiling is a nice complement to the random method, and it can be adjusted upward and downward depending on new information and training, and as I mentioned, it can be applied to those evading as well as those going through voluntary screening. Canines are also promising. Teams trained to sample people have had good results in one system, and I think it's something that should be explored. Lastly, we need to be able to deal with vague threat information. You need to press these agencies for information; when you get an answer that says, well I can't tell you, keep asking them. The public has a lot of misunderstandings about intelligence I think they always think that everything we do has specific intelligence that can be conveyed, and we know that's not true. So they tend to mistrust what you're doing, and that puts you in a difficult bind. And, so, here's a menu that we came up with. I'm not going to read these, but they're in the report and they're a good starting point. Notice the last one: if it's not credible, you don't have to do anything, which is sometimes very hard to do. It's often harder in security to do nothing than it is to do something.

These are the capsules of what makes a good screening process: high probability detection, maximizing deterrence, contingency plans that allow you to expand and contract, screening that's fully budgeted, passengers and the public who are actively engaged through a program of public outreach and education, and field-deployable technologies that have been tested in real operating conditions with protocols, and training. You need a set of policies and procedures that flow down to protocols you train on, and the training must be continuous. You need a program of quality assurance which is used to make sure that the program is doing what you intended it to do. All of this will not go anywhere unless you have first-line supervisors who are motivated, care about their people, are true leaders, and who have top-level agency support. Gravity is one of the most important forces in management. If you have courage at the top, it will flow down. If you don't, that will flow down as well. Thank you, and with that, I'm going to turn it back over to Brian.

**BRIAN MICHAEL JENKINS:**

Let me just take a couple of minutes here to wrap up. Bruce mentioned a couple of times the problem of vague intelligence and threat information. When it's over, when we go from green to yellow, or yellow back to red without explanation, it's not a matter of people withholding information. It's just that a lot of times that information is not available. One approach to this is to have an internal management discussion to make the continuation of any measure the consequence of a positive decision. In other words, you say, we are implementing these new measures and these new measures will automatically expire in ten days, two weeks, whatever it is, and at that time, unless we have additional arguments for continuing these measures, they're going to come off. The problem is that we don't know when to lift additional restrictions and security measures. You will have to set an arbitrary date that says "this will come off unless we decide positively that it must be continued."

Certainly, we agree that mass transit surface transportation is an attractive target. We know that 100 percent screening isn't feasible. We do, as we have indicated here, believe that selective screening is a viable option. We know that a realistic goal is not prevention. It is risk reduction. We know that current technology can be of assistance, it can facilitate, but there isn't a silver bullet here. We don't have a technological solution to the problem. We do know that selective screening bumps with our national psyche; it's not what people like, and therefore, the

implementation of any program is going to have to be very carefully crafted and controlled to avoid sliding into anything that is misunderstood. We know that, despite your best efforts, there will be legal challenges; that is the way democracy works. However, we believe that these measures will be upheld in court, but only to the extent that they are well-crafted, well-designed, and well-managed, and that you can make a convincing case.

The convincing case does not have to be made on the effectiveness. That's an interesting aspect of the decision in the court case in New York. The judicial branch has said, "Look, it is not up to us,"—meaning us, the public, or us, the courts—to determine the effectiveness of the security measure. What is up to us and the courts is to evaluate whether or not it violates the Constitution, whether it violates the rules, because part of the challenge was that it's ineffective, and the courts took the position—a very conservative position—that effectiveness is a decision for the security operators to make.

The bottom line is that these things work well only to the extent that the public is engaged in them, and that means if there's going to be any selected screening process, it's going to have to be accompanied by a vigorous public education program to say what we're doing and what we're not doing here.

You need to plan your system now, not when the next bomb goes off somewhere in the world, and you're obliged to ramp up security fast. That's not the time to do it. The time to do it, the planning for it, and the thinking about it, is now, so you have something ready to roll. It's going to require a lot of management and a lot of public education to make this work. Thank you for your attention. We will both be around during the break for questions, and you'll also have a chance for more questions with other panel members this afternoon.

**ROD DIRIDON:**

Thanks, Brian. Let's thank these two fine experts for sharing their time with us. You folks are the leaders of the national transportation security community, and some of you have been dragged kicking and screaming and some have come here very happily and voluntarily to be with us today. So we're going to set up a time after the secretary speakers for an in-depth discussion. You can ask our speakers questions, and they may have questions of you too. We'll have not only these two gentlemen but also Secretary Mineta and Secretary Chertoff for the after-keynote panel, joint panel, and speakers' session as well.

So we're going to hold the questions until that time, if you don't mind, and we'll take the Q and A as long as you want to stay in the afternoon. In addition to the secretaries, we'll have Mort Downey, deputy secretary of transportation for two administrations, and he'll be here for the introductory processes.

**BILL MILLAR:**

Now we have a panel to begin to explore the topics in a little more detail and from a number of different perspectives, and I'm extraordinarily proud that this panel is chaired by my director of security, Greg Hull. Greg is someone that I believe just about everybody in the room knows and has worked with. He gives staff support for all of our security activities, along with Vaveen Williams, who is also here, and had a hand in developing and shaping APTA's safety programs. We made a recent decision to split our safety and security programs, and Bill Grassard has become our director of safety. Greg is also responsible for our peer review program and for our rail, bus, commuter rail, safety and security programs, and he acts as our industry liaison on security matters with the Department of Transportation, the Department of Homeland Security, the Transportation Security Administration, and the National Transportation Safety Board. Greg came to APTA in 1999 and has over 25 years of experience in public transit operations and management. He's a graduate of the University of Manitoba and the University of Calgary; he's a registered safety professional and has many other additional credentials in system security and safety program auditing. Please join our panel moderator and let us welcome Greg Hull.

**GREG HULL:**

Well, thank you very much, Bill. And welcome back everybody, and my appreciation to the Mineta Institute and to Rod Diridon for putting this summit together. Many of our transit systems base their security on people, procedures, information sharing, and strengthening our infrastructures through a variety of means, including technology resources. However, our capabilities for security are also tied to the level of funding and resources that are available to us. Screening, which is the theme of this summit, is one of the methods we use in a systems approach for security. And while there is no question that well-trained personnel are a foundation for effective security, we all know that we simply don't have enough cops and dogs to throw at these issues, so we also look to technological tools to use. But we wrestle with these tools in trying to determine what works, what doesn't work, what approaches are cost-effective, and how

we can blend and meld these resources and approaches together into a sound strategy that we can use in our transit agencies.

Now, I have the privilege of knowing each of our panel members. All of them have provided critical leadership for our industry in our post-9/11 security initiatives, and they bring to you their own unique perspectives. The distinguished panel that we have includes Colonel Douglas DeLeaver, chief of police with the Maryland Transit Administration; Ron Frazier, director of the Office of Public Safety with Newcastle County and former chief of police with Amtrak; Robert Jamison, the deputy administrator of the Transportation Security Administration; and Polly Hanson, chief of police right here with the Washington Metropolitan Area Transit Authority. It is my pleasure to introduce our first presenter, Colonel Douglas DeLeaver, Doug is a 37-year veteran of law enforcement for the state of Maryland, and has been twice appointed to the rank of colonel as the Chief of Police for the Maryland Transportation Administration police force. Colonel DeLeaver is assigned to the governor's Homeland Security Task Force and is a prominent member of the Maryland Emergency Management Agency. He's also an advisor to the President's Homeland Security Task Force. Chief DeLeaver has traveled to Israel to participate in international security programs, and to London to evaluate their citywide surveillance system and the security measures implemented since the 2005 subway and bus bombings. Doug is a graduate of the FBI National Academy and holds a Bachelor of Arts degree in Criminal Justice, he's a graduate of the Miami Dade College of Assessors for law enforcement, he's also a certified instructor in numerous law enforcement subjects and is a frequent speaker at transportation security and public safety workshops. Please welcome Doug DeLeaver.

**DOUG DELEAVER:**

Good morning. I'm in charge of the Maryland transit system, and I took public transportation this morning. I took the train, and I observed one thing when I came across this morning, even though it was dark, I didn't see any flags waving, nothing over foot passes—people waving flags like they had been after 9/11. So, it shows you that we've gone to sleep. We don't believe anything is going to happen in transit. We know it's probably going to happen, but we've all been lulled back to sleep. The community wants to know what we're doing in transit; it was on TV last night because they wanted to know what crime was on our light rail system. But one

thing I want to start off saying. We were committed before 9/11, in transit. We were committed. We were already protecting our system. I sit on the APTA transit security, and we've been doing things for a long time—long before 9/11.

The Maryland Transit Administration police and the Maryland Transportation Authority have demonstrated through their policies that they protect their system. We have the ability to seamlessly and effectively implement new proven strategic programs. Some of these programs came after 9/11. When TSA came in, we got canines, but while they gave us a 16-point process that we had to do, they didn't give us any money to do it. They came up with a matrix of threat conditions that we had to abide by, step-by-step standards. When the threats went up in colors, we had to do different things. The State of Maryland had a homeland security director, and on this basis we continued to partner with the joint terrorism task force, TSA, the Department of Homeland Security, and the Intact System in Maryland (the coordination analysis center which filters all intelligence through it). We did a local and state response system because the local people are the last ones to find out what's going on.

We have a TOC, which is a Tactical Operations Center. It goes up when anything in transit occurs. As a result of the London bombings, law enforcement in New York implemented a program of randomly checking baggage for patrons utilizing rail in mass transit systems. New York City is faced with a number of challenges. The New York public transportation system, including both bus and rail, moves some seven million passengers daily, with 24 billion New Yorkers using it yearly. About one in every three users of mass transit in the United States, and two-thirds of the state, rides their system. New York and New Jersey have a history of terrorist attacks and threats, as al-Qaeda's community have specifically targeted these areas. New York City has been a target of terrorist operations including the 1990 assassination of Rabbi Kahan; the 1993 landmark plot against the Holland and Lincoln tunnels; the 1997 attack against the New York subway system; in 1993 and 2000, attacks against the World Trade Center; and the recently uncovered plots against New York Stock Exchange and Citicorp Center in the summer of 2004.

I relate to these threats because it affected us all in transit. Maryland faces different challenges in homeland security. The Maryland Transit Administration is a bus-based system, with a daily ridership of 231,000, which comprises about two-thirds of Maryland transit ridership. The MTA

metro has a daily ridership of 46,000 people, the light rail closer to the 29,000, the Marc train, which I rode this morning, has 24,000. At the present moment, the Maryland Transit Administration police force and the Transportation Authority do not view tactics of random bag searches as the most effective tactic. Based on intelligence and intelligence-only reporting, MTA police and the MDTA police are prepared to conduct random searching, if necessary, if it's going to prevent the public from having fears, things like that. What I noticed this morning was that everybody on the train had a bag, everybody had a computer, or a knapsack, and I ask you how many people got searched when they walked in the hotel this morning with your computer bags. Nobody searched you, but if you were in Israel, they would search you, they will search your bag, and they will search your person.

We have policies for random patrols and what we call Operation Zeus, which is zoned, enforced unified sweeps, where there's a surge of our officers that go into the station. We use mirrors, we use canine dogs, and we go in with lights and sirens. It takes about three minutes. We stop the train, board the train, talk to the passengers, clear the platform and we're out and then we critique what we do. So it's a surge that we do all the time. We do it at Amtrak when they call. The Maryland Transit Administration police force, and the MDTA, which is the Maryland Transportation Authority responsible for securing all infrastructures in the state of Maryland, are responsible for all of the Park & Rides, the train stations, the bus stations, everything that moves on rail. The random searches we're currently doing already strain our current resources. If we had to do bag-by-bag, we couldn't do it as effectively. We couldn't do it at all. In addition, it frequently involves profiling, because you have to pick the people and train the people, like the speaker said. If you don't train your employees to do what they're supposed to do, they'll do random things and they'll do something wrong, and you're held accountable.

We may delegate the task, but the responsibility stays with me 100 percent, so the employees out there that are doing it, I'm responsible for their actions. We have 14 metro stations, 32 light rail stations, and 42 marked stops that would divert resources from our critical infrastructures. We have the BWI Thurgood Marshall Airport, and the Port of Baltimore, and all the bridges and tunnels in the state; we also have an officer-on-board program for our rail system.

We have a program where we send plainclothes officers who ride the system from the outskirts of Maryland into D.C. That's our eyes and ears. They sign a pledge sheet that says if something

happens, they will be responsible and take law enforcement action. Each month we send them a ticket back, they ride gratis, so we have over 200 onboard officers that do this. It's a great program, and they love it. Federal agencies looked at it at first and said, no they can't do it, but they're doing it anyway. They're riding the system. So we let them ride it for free, and you show your ID, we'll let you ride on this onboard program. The only thing you have to do is sign it each month. We'll send them a ticket so they don't have to identify themselves to the conductor.

Department of Homeland Security administration and the FBI have made a number of recommendations to improve our rail security, but I say we've been improving our system all along. But we still have to respond to the federal mandates and the advisory they issued July 7, 2005, that when the threat levels are increased to orange for mass transit and rail we have to do certain things. Both the FBI and the TSA have not recommended the random searching of passengers. The Department of Homeland and the Federal Bureau of Investigation stated that they have no specific credible information about any terrorist threat in the U.S., something that was brought up by our two speakers when they suggested that an attack in the U.S. was going to happen.

You know, we talk about bombings on our system. The first explosive device was used in September of 1920 in New York. The individual was vengeful, against J.P. Morgan and Co. He took his horse-drawn wagon down at Wall Street and Broad Street, and he blew it up and killed forty people. The first suicide attack was carried out in 1983, and that bombing was the bombing in Lebanon of U.S. troops. So you have to look at it. They have been doing this for a while. It just didn't start happening. Mostly we find from intelligence, that terrorists look at nightclubs, they look at malls, they look at places where young people gather, because, we figured—when I was in Israel, they said young people are normally not as cognizant of what they're doing if they're in a setting like a carryout or a dance or something like that. Railroad stations and airports, these types of targets are always attractive given the number of people present. Even when security detection mechanisms are employed, terrorists can still cause higher numbers of casualties by detonating entrances of these locations. What I learned from intelligence and sitting at these security roundtables, especially at Johns Hopkins, was that top-fifty targets are restaurants, malls and shopping venues, because a lot of people go there. My greatest fear in Maryland is that terrorists are going to blow up a school bus with kids in it. Something like that would get the maximum amount of attention, there's no question. They don't pick holidays, they

don't pick anniversaries. They may say today, the fifteenth of March, five years from now, we're going to blow up a hotel, and that's what happens.

We have an assistant U.S. Attorney in Maryland, Harvey Eisenberg, who stated that random searching of transit patrons' bags is not an effective use of law enforcement resources. This has been our understanding of random searches as well. The best tool we have are the officers that are working 3 to 11, 7 to 3, or 12 to 7, on that street. We train our officers to find out what's going on. It is responsive personnel, not technology, which will help create a secure transit system. I'll give you an example: when I was in Atlanta, we had fare inspectors on our system because of fare evasion. One of the fare inspectors found a note on the seat which had the president's name on it and some other things, and they called the Secret Service. They were so taken with it, that they upped the presidential protection detail for about two weeks. So people, not technology, are going to provide real security. We had a special machine in Maryland with a fingerprint identification system where, when you put your finger on it, or money in the machine, it would tell you when someone had touched explosives, but only after-the-fact. I went to London and looked at a camera system that's very elaborate, but it's not going to tell us if somebody is carrying a package. But if something happens, we can only go back and look at where the alarm went off, and at what happened. While this is important—and we should have that up and running in Maryland by September—the best prevention that we have is a personnel strategy.

You have to be able to plan for anything and everything. The Israelis always emphasized that the best strategy is based in prevention. Israel is about the size of New Jersey, and the Israeli police have 30,000 officers on their payroll, and 70,000 volunteers with their ears and eyes all over Israel. Their goal is to get a subject before he leaves his or her residence, not when he or she gets to the checkpoint.

The public can help in most critical areas. We need to train our maintenance people, our people down through the entire system, to be lookouts, so that if they see something out of the ordinary, it is reported immediately. We had a young lady working for the transit department go to Lexington Market one day and get a fish sandwich. She opened it up, and she took the sandwich out and noticed white powder. She called her supervisor, then she called the fire department. They came, the HAZMAT team came, they looked at the sandwich, they did a chemical test and

found that it was cornmeal from the fish sandwich. We had one of our officers who had a headache, and he opened this headache powder, and he left it on the desk, and a supervisor came and saw it. He thought it was anthrax, and we had to clear the building, and while that's an embarrassing situation, at least somebody was looking.

Some of the strategies I talked about, such as Zeus, we have TSA training dogs, we have a mobile command center, which cost about \$1.2 million. Our tactical operations center has coordinated efforts for law enforcement for most counties throughout the state. We have a special program of undercover officers dressed as homeless people, who the press is always trying to discover. We've also taken some things from Polly's shop. We have a behavioral pattern and recognition program. DHS has a funded grant program for recognizing behavior characteristics, called SPOT, and the training has already begun. The JTF investigates all reports of possible suspicious activities that may be related to terrorism. They have investigated everything that has happened in Maryland. Our transit police and transit authority have partnerships with other law enforcement agencies and continue to look at ways to improve what we do. APTA's been a great help, and we will continue working with TSA, DHS, and FTA and APTA.

I've been doing this for 38 years, and my system is safe. And if a terrorist attack does occur, we'll be prepared to go because we've been training for a long time. Thank you.

**GREG HULL:**

Well, thanks very much, Doug, and thanks for persevering through that cold that you're fighting off. Colonel DeLeaver has reminded us of the importance of a number of things relative to security, and one of those things is that everything has to have an acronym. Zeus, of course, which many of us are familiar with and that many of our retired colleagues used to refer to quite a bit. If some of you don't know what the CASE method is, it means "Copy and Steal Everything." The ability to copy is a wonderful thing within our industry because it highlights the importance and the value of sharing practices and programs. Chief DeLeaver noted the Zeus program, as well as highlighting his sharing plans with New Jersey transit and with Washington Metro.

I know that next time I'm going up to Baltimore and I'm using the system, I'm going to be looking twice for those people that appear to be homeless, so thank you for sharing that with us.

Our next speaker is Ron Frazier. Ron started his career in Army Intelligence and then spent five years as a police officer in Maryland before joining the Amtrak police force. He served with the Amtrak police for more than 20 years, working his way through the ranks from captain to chief of police and security. As Amtrak chief of police for more than ten years, Mr. Frazier led a national force of 350 officers, led the agency's emergency planning and homeland security effort, and provided oversight for the agency's emergency communications system. Since 2004, Ron Frazier has served as special assistant to the U.S. Department of Health and Human Services, assisting the department's emergency public health and security planning efforts nationally. In July of 2006, Ron became Director of the Office of Public Safety for New Castle County in Delaware, where he works to protect the health and security of the people in the first county of America's first state. Please welcome Ron Frazier.

**RON FRAZIER:**

First county, first state. That's good, I like that; thank you. Good morning. My first part of business is give you all a legal disclaimer since I'm going to talk about legal issues. I have actually been suffering from vertigo over the past week or so from an inner ear inflammation, and so I'm disclaiming anything I say to you here today as being a direct result of that illness. I'd like to start by first talking about some of the things that have preceded me. The Mineta Institute has been involved in security matters for a while, and I first came to work with them in 1995. Rod Diridon pulled me out to San Jose in 1995 after the Heider train derailment, which was an Amtrak event that occurred in October where we lost a person—a gentleman by the name of Mitchell Bates—in an act that has never been solved. Credit was taken by some person or persons who identified themselves as the "Sons of Gestapo." That was an incident of domestic terrorism on the rails of the United States, and that's how I first became involved in a significant way in matters associated with terrorism.

I'd also like to talk a little bit about the APTA, William Millar, Pete Kanedo in the public safety committee, and Bob Herton. They've all been involved for years in these issues. From our perspective, those groups have been critical in assisting us in terms of security, and there's a third group, who I'm here to talk to you about today: the Transit Cooperative Research Program. There is a book that I have had the opportunity to be involved in, called *Public Transportation Passenger Security Inspections: A Guide for Decision Makers*. This book is currently in the final

stages of peer review, and hopefully we'll successfully get through that process, and it will be available to you sometime soon.

I'm going to talk out of that text a little bit about legal issues associated with passenger screening. A little bit earlier, Brian Jenkins talked about the effectiveness of inspections and how that wasn't the real legal issue. I thought that was well said and relevant to the concepts that we're dealing with. When it comes to legal aspects of what you have to get done, most of these legal issues are going to fall under the fourth amendment to the Constitution. The reality is that the fourth amendment is going to apply to government conduct as related to search or a seizure. A seizure occurs when a person's liberty is restrained either through physical force or show of authority. It also only attaches when the person searched has a reasonable expectation of privacy, and therefore a transaction in plain view, in a public forum, is not normally subject to the fourth amendment protections. That's why video cameras that are placed in your stations don't come into conflict with the fourth amendment. For the most part, these searches are going to come clearly under the fourth amendment and state constitutional provisions, which, absent probable cause or a warrant, can only be justified as an exception. And that's the context that we need to operate under in terms of searches or screenings.

There are a number of methods for passenger screening that are out there. The first is manual inspections, which typically involve the random selection of transit passengers and their bags. The officer may open the bag and visually inspect the contents; manual inspections relate to an officer actually moving contents within a bag to reveal hidden items, opening up or unzipping pouches. From a safety perspective and an operational perspective, who do you want going in that bag? Do you want the would-be terrorist going in there to move stuff around, or do you want the officer going in? It's the kind of thing that you have to think about, in terms of your decision making when you're setting up these programs.

This all started as has been mentioned previously, in July of '04, up in Boston, when that city became the first in the United States to conduct visual or manual random baggage inspections. They were done by the MBTA (Metropolitan Boston Transit Authority), as I've mentioned. They were in response to concerns about the Democratic National Convention. Then in July of '05, they also began these random inspections and used these methods in New York City and the New Jersey Met area. Of course, there were legal challenges. Neither was successful. This

establishes a precedent for how we can proceed. This means that, generally, random passenger inspections can be legally justified under an exception to the Constitutional warrant, the requirement is that it has to be designed to meet a substantial governmental need, no more intrusive than required, subject to neutral criteria, reasonably effective, and aimed at an objective other than general law enforcement. If you meet those criteria in the establishment of your manual searching system, then the random inspections should pass muster.

The next type of screening uses technology, an area where there are more complex laws. The technology of the inspections is pretty much the kind of thing that you're going to get at an airport, metal detectors, x-ray machines, etc. Some of these include complex issues that you have to think about: intrusiveness, privacy concerns, and claims regarding unreasonable detention. You can't forget the health risks associated with radiation, although it may be in modest or small amounts.

Some kinds of things, such as a trace detector, are integrated in a ticket machine, and although it's not that intrusive, it might make sense to set up a legal system that can back it up. The other thing that you have to do is ensure that a secondary inspection mechanism is in place because technology-based screening is not going to get you end-results. They are a beginning point for further screening and searching.

There are other associated-technology inspections such as the back-scatter X-ray machine, which was mentioned by Bruce Butterworth. This is the one that can kind of see through things; you have to be really careful about implementing something like this from both a privacy perspective and an intrusiveness perspective. What you want to make sure is that a screening or a possible detection isn't treated as evidence of guilt. - This is, again, something that requires secondary screening before you reach any conclusions. When I worked on this issue from a perspective of detecting drugs, and many of you have been involved in that kind of activity, you know that you may hold the bag but not the person, for example, because a lot of legal issues have more to do with avoiding any problems associated with unlawful detention.

Canines are something that you can put in place. Canine explosive teams are a part of the security scheme for many agencies in transit, but there are a few things about canines that I want to talk about. One thing is that you need to be cognizant of the potential for a dog to bite somebody, so please do not forget that in your planning. You need to review state laws regarding

that. Another thing: the in-house program will generally have greater liability than a contracted service in your policy planning-level decisions. Meeting federal certification and training standards can reduce the risk of liability, and in setting up your search policy, you should clearly state the authority for the program, document performance standards and establish your use of force and invite policies. On the Constitutional end, to ensure that the inspections are reasonable under the fourth amendment, care should be taken to not associate explosive detection canines with regular law enforcement.

The final section I want to talk about is one that has also been mentioned previously and which involves screening based on behavioral assessment and observation of passengers. The BASS program is a behavioral assessment screening method, and SPOT is another one. In these systems, what you're doing is observing specific behaviors of passengers, which may include questioning and identification checks. In conducting screening of this nature, there are two legal issues that may arise. The first is whether it is reasonable for any resulting search and seizure under both federal and state law. Keep in mind that this is as it relates to racial profiling. There may be more stringent regulations or more stringent laws in existence that require that you pay particular attention to what's going on in your local jurisdiction. The other, of course, is the fourteenth amendment challenges against racially based screening. In this second challenge, there do not appear to be any recent decisions. There is one case that we're watching, it's in pre-trial status right now: *Downing vs. Massport*. The plaintiff is basically alleging he was unlawfully detained at the airport by state troopers, threatened with arrest, asked for identification, etc. Although it isn't settled, it gives us the allegations of the plaintiff and an understanding of what kinds of things we need to be concerned about.

The main allegation (and they use the BASS system up there, at Logan) is that the BASS training directs state troopers to stop, question, and/or arrest certain individuals at Logan, despite the absence of reasonable suspicion, and that it authorizes state troopers to deny access to Logan to persons who refuse to cooperate with their request for identification or other information, and that the policy effectively condones and encourages racial and ethnic profiling. The *U.S. vs. Martinez-Huerta* is also a seminal dissenting opinion: that the use of one's ancestry as suggestive of possible criminal conduct is repugnant under any circumstances.

That's the concept and where it starts, relative to dealing with racial and ethnic profiling, but where do you get the reasonable suspicion standards? Well, we use them in hijacker profiles at the airports, and reasonable suspicion came to prominence under Terry vs. Ohio, which said that it rests on the investigating officer to find specific reasonable inferences. He or she can make these based on the situation, in light of his or her experience.

These criteria for reasonable suspicion are subjective, but whether we're using subjective or objective criteria, the amount of discretion exercised by the police and the amount of training afforded by the officials are important. Behavioral assessment includes objective indicators such as interest in operational details, or it relies solely on subjective indicators, such as appearing nervous. Discretion is typically afforded to the inspecting officer; however, whether a person who declines to provide information would be detained, asked to leave the system, or have no further action taken, or whether the protocol includes questions designed to confirm or dispel suspicion before further action is taken, and whether the behavioral assessment we used to move passengers will reach a certain threshold to secondary screening are some of the issues that you want to determine in establishing what the reasonableness of a search actually is. If you have questions a little later, I'll be pleased to take them, and I thank you for your attention.

**GREG HULL:**

Thank you very much, Ron. It's interesting that the piece of research that Ron was working on came about as a result of a lot of people in our industry—general managers, heads of security—wondering about the legal implications of conducting searches. For those of you who are wondering, you can access the report through the Transportation Research Board, and through the APTA Web site. You just need to click on the APTA Web site, APTA.com, go to TCRP, and you can access all of the various TCRP reports. As you heard earlier, our president, Bill Millar, serves on the oversight committee for TCRP research, and I should also point out that our next presenter, Robert Jamison, during his watch, with the FTA, supported a variety of measures to increase security, including the provision of \$2 million towards transit security research to be conducted through the Transportation Research Board.

So when you go to the Web site, you'll find a number of different resources, including the piece of research that Ron referenced. That leads me to our next presenter, Robert Jamison, deputy administrator of the TSA. Robert was appointed deputy administrator of the TSA in October

2005. Previously, he was a deputy administrator of the Federal Transit Administration, appointed by Transportation Secretary Norman Mineta. At the FTA, Mr. Jamison spearheaded the agency's Transit Security Program and its \$4.5 billion Lower Manhattan transportation recovery operation. In 2003, he was awarded the Secretary of Transportation's 9/11 Medal, and in 2004, he received the Department's War on Terrorism medal. In January 2005, President Bush designated Mr. Jamison acting administrator of the FRA (Federal Railroad Administration). There, he directed the development and implementation of a data-driven national rail safety action plan. Robert is a Magna Cum Laude graduate of the University of Memphis, with a Bachelor of Science degree in electrical engineering. Prior to joining the government, Robert was a senior operations officer for the American Red Cross and in management at United Parcel Service. I'd also like to point out that during his tenure over at the FTA, many of the programs that have emanated through the FTA, that TSA now partners in, were a result of him being involved and giving authorization to move forward.

We had a very strong partnership with him and his staff over at the FTA, and we are building a very strong partnership with the TSA now, so please join me in welcoming Robert Jamison.

**ROBERT JAMISON:**

Thanks, Greg, that was a very kind introduction. I want to start out by thanking Rod for the invitation and to thank the Mineta Institute for hosting this. I also want to say that it's quite an honor for me to have served under the extraordinary leadership of Secretary Mineta. Having been afforded many opportunities, such as the FRA position, with his confidence, it's an honor to be here, and I'm glad to be part of this seminar.

I'm fully aware that the focus of this is passenger screening, but I want to take a little time to talk a bit about our priorities and some of the things we're working on at TSA, and I promise to hit the screening issue because I think it's important. I'd like to say that I agree with almost all of the recommendations and findings of the white paper, but I want to take some time to talk about our three top priorities. They're high risk, high consequence, and I'll talk a little bit more about them. We talked a lot about screening, we talked about random screening, and we talked about search teams, about Zeus and Hurricane teams. We at the TSA believe that visible, unpredictable deterrence is one of the best measures that you can take in mass transit, and it's a concept that

we're utilizing in aviation. Our priority needs to be raising the baseline of security and focusing on the fundamentals.

High risk, high consequence. Brian was talking earlier about the history of the attacks in Madrid and in London and what we've learned from those attacks. When you go back and look at it from our perspective, we put a lot of focus on high risk and high consequence, particularly in the grant programs. We look at high-passenger or -density systems, with underwater or underground infrastructure, and we talk about the consequences of attacks. There are dramatically more consequences underwater and underground. We talked about the impact of explosives in a tight tunnel environment in London, and when you compare it to other aboveground attacks. In Madrid approximately 200 people were killed, and it was largely an aboveground attack. But when you compare it to the level of attack in London, I'm convinced there would have been dramatically more casualties if that level of attack had taken place in an underground infrastructure, because underground infrastructure dramatically magnifies the impact of an explosion. It dramatically complicates the response effort, the evacuation efforts, and it also creates a higher threat level for the non-ID attacks such as chemical and biological in that environment; thus, underground and underwater need to be our primary focus when it comes to security.

If you look at Madrid, roughly 10 times the amount of explosive was used in Madrid versus what was used in London; those are some rough comparisons but it gets to the point that there could have been dramatically greater consequences had it been underground. The system was up and running in Madrid within 48 hours. The London system was down for a much longer period of time, closer to months for the Kings Cross line. So in addition to greater human consequences, it had a much greater economic consequence.

We at the TSA spent a lot of time focusing our grant funding and our mitigation efforts on mitigating areas with higher risk and greater potential for consequences. We restructured the grant program over the last few years and had a tier-one structure, which held high-risk properties, and a tier-two structure with mid-level-risk properties, with the majority of the funding going to those higher-level risk properties. We determined these locations by factoring in passenger density, underground and underwater infrastructure, and we're going to continue to

try to make sure that that money is driven towards mitigation projects that are doing the risk reduction.

So, as we build a formula, we're going to be trying to work more with the industry and the grantees to make sure that we're trying to address those risks in those tunnels. There is a tunnel working group that has been formed over the last six months which has been doing a lot of research. The TSA is also involved in some of the early vulnerability assessments with the FTA, and a lot of the transit agencies. They're doing vulnerability assessments on tunnels and other high-risk infrastructure. There have been multiple federal agencies that have been involved in this project, including the DHS Science and Technology Directorate. We pulled all of those entities onto one working group, tried to come up with a coordinated and consolidated approach to assessing the vulnerability, to make sure that we truly understand the vulnerability of those assets.

The next thing I want to talk about is visible unpredictable deterrence. I talked about that a little bit earlier, and we've all talked about the magnitude of the responsibility and the magnitude of the passenger load. The fact is, we can't screen 100 percent of our passengers, nor should we ever try to do that, with the amount of overhead and economic consequence it would have on our systems. However, we can provide more visible unpredictable deterrence: the Zeus teams, the Hurricane teams, and other search teams. This concept is something that we're applying to aviation, so if you follow aviation security, as the debate moves from checkpoint screening to air cargo screening to airport employee screening and all of the fronts that you have to move, we very much believe that we're getting a flexible force that can move randomly throughout the environment. This force can create unpredictable deterrence, and the terrorists cannot know when or where they may encounter a different level of security. You have to balance that with the customer needs and the passenger needs on airplanes, but the concept of "random and unpredictable" has worked well, and we really try to drive that.

We're doing it through the canine program, and we plan to have 56 canine teams by the end of the year; I think we've got 45 and we're pushing another 11 through the training process this year. We are proposing in the president's budget that we should have an 80 percent increase in that process, and drive another 45 teams to the next fiscal year. We have Viper teams, which involve a surge and being able to apply our resources. At TSA, we do have a lot of resources,

and we have a lot of resources that are primarily associated with aviation: 43,000 TSOs and a large number of federal air marshals. We also have 47 other deployments across the country with other modes of transportation, including mass transit, and we wanted to continue to increase that. We think it provides a good use of our resources to put that unpredictability, that visible deterrence, out into that environment.

When we help, it's always at the invitation or with the direct assistance of the local law enforcement or local jurisdiction, and it provides a force multiplier. What we really hope it does for us is build relationships with local companies, so that, for instance, when we do have a specific threat in a specific system, or something that we would want to respond to, we've already got relationships and we would be able to surge our resources into that area. We've got a few more deployments scheduled and, actually, we've had a few high-profile transit agencies request assistance recently, so we're encouraged by that, and we think it's a valuable resource.

The last piece is to look at operational protocols, some of which we have already talked about. I'm going to talk a little bit more about it going forward, but we feel like an important role for us is to try to give guidance and to try to glean the best practices from around the industry. We watch what transit agencies are deploying: Zeus teams and other visible, unpredictable deterrence. We watch agencies to see how they feed current assets.

Raising the baseline of security means augmenting three primary areas: training, public warnings, and emergency preparedness. That's what has been focused on at the FTA, and it's what we're trying to focus on at TSA. We're working with our Peer Transit Security group to get feedback on whether or not we've got the top priorities properly assessed, we've asked for self-assessment by the largest transit agencies of where they stand on "the 17"—the top 17 priorities for mass transit. We're trying to determine how well those fundamentals and the key security issues are implemented, and we're having that drive our grant process.

Training is a fundamental priority, we've talked about how open the systems are, and how vulnerable the systems are, and we've talked about how difficult it is to protect them, and you've got to be prepared to respond. Your front lines are your employees and the people that are riding the system and since 9/11 there's been a lot of effort focused on training and informing employees and system riders. Based on the efforts that I talked about earlier, with regard to our inspectors and the self-assessments, the early results are not exactly what I would call

encouraging. Without going into a lot of detail, what they're showing is that after 9/11, we had a big push on training, but a lot of the recurrent training and refresher training is not being done. So we're trying to remedy that situation, because I believe that the best return on investment you can make for transit security is to make sure your employees are properly trained.

After 9/11, security training was a major focus at the FTA. There were several transit agencies that were being very aggressive with their training. The industry asked for more guidance and more programs, so we worked with NTI (National Transit Institute at Rutgers), and we worked with the system to try to develop a training program that we could send out across the country. Very quickly, we learned that one size doesn't fit all. You've got a two-hour course, I've got 15-minute increments, I've got labor rules, I've got issues, I need flexibility. So we spent a lot of time and effort trying to break it up, give you lots of options, give you videos, give you 15-minute programs, to give you the flexibility to still train your employees despite difficulties. I think the NTI courses have achieved a lot of that through the good work of the FTA.

The next big hurdle was: I have a work force of 43,000 security officers, and to be able to have the time to train them we've got to pay them overtime, and we've got to take them out of service. This presents a huge challenge, so we worked on trying to get funding flexibility through SAFETEA-LU and the transportation re-authorization bills. There's flexibility built into the 1 percent takedown on the formula money for transit agencies to spend on training. The DHS grant process was changed to allow overtime and flexibility for training dollars, yet, even then, funds are still tight so we try to offer more specialized streamlined training. For example, if it's a frontline employee or a train operator or a station manager or a supervisor, we recommend a certain type of training. Our training falls into some broad categories, from awareness training to national response training, operations center control training and five other broad categories. It's also broken down by employee type. We set up the '07 grant process to dramatically streamline the availability of funding for training. So instead of having to go through a large justification process, we've come up with a menu that says we will pay or reimburse "x" number of dollars per person trained. You fill out that form for how many people you'll train and we'll try to get the money to you based on need. So we're trying to really get the training out there, because we feel it's most important.

Now a little bit about screening. I said earlier that I agree with the majority of the findings from the White paper about moving from purely random to more selective screening. I base that on what we know. We've talked a lot about the openness of the system, and the 1500 people per minute, and the difficulties in screening. One new point of reference that I'd like to address is that I got the opportunity to go to India for a rail security conference following the attacks in Mumbai, and the railway minister there tried to implement a 100 percent screening on India railways after that event. I learned a lot about India railways, which is the largest railway system in the world and is the largest employer in the world, not just rail employer, but the largest employer in the world. Yet even with a security work force 60,000-strong they cannot do 100 percent screening. They disbanded the 100 percent screening attempt in a matter of hours.

I have talked a little bit about the attack history, dealing with consequences of an attack which is underground and/or underwater. But the other big piece about the attack history is that in London, knowing that on July 7 the terrorist attack caused a height of concern and alert, there was still another event on July 21. This attack would probably have been successful if not for the composition of the bomb. So even with that heightened alert in trying to prevent this, and with all of their resources, it could still occur.

Another point about attack history that I want to make is that I have watched the mass transit security discussions and some of the funding decisions that transit agencies have had to make. There are tradeoffs in those decisions. There have been a lot of discussions about where to put money, and there have been a lot of discussions about back-end security and front-end security, and largely what I've seen from this is that they're still attacking us through the fare gate, and they're not attacking us through rail yards or through insider threat. That leads me to believe that using visible unpredictable deterrence is good because that's your best defense from the attacks through the fare gate. We talked a little bit about the research and the technology, and I said earlier that I agree with the overwhelming majority of the white paper findings. The one caveat that I would have on those issues is I'm a bit more optimistic that technology can play a role in the screening process.

This is something that came full circle for me because I very much had the same findings that your paper had as more of the results have come in from TRIPP and the PATH pilots. Of the two PATH pilots, one was an aviation screening-type pilot trying to put aviation security into the

transit environment, the other was a more aggressive technology which used millimeter wave, infrared, and other screening technologies. We've also done some mobile explosive detection technology, or handheld mobile explosive detection, and we're currently doing another handheld millimeter wave standoff detection pilot. So while I agree, that there is no silver bullet for technology, I think that there are things that we can apply to do a better job of implementing screening should we choose to do that.

Until then I think we can take what we've learned from SPOT, our program that we've got in the aviation sector and that we started in Logan airport in Boston. When we first rolled out this behavior-detection program, which is largely driven by the detecting signals in behavior and mannerisms, about 95 percent of the people that were targeted by that process were confirmed to have been hiding something. So I mean it wasn't necessarily terrorists that we caught, but we caught several people that had expired visas, fake IDs, etc., at a hugely successful rate. So the ability to do that type of behavior-pattern recognition is a method that has been validated. How to do it in a much higher-volume environment, such as mass transit, is something we're working on, but to apply that principle in connection with some technologies has promise.

I think there's a capability to overlay currently used techniques with future technology to create a much stronger grid for protection. So, with that I will take my cue to get off and make way for the secretary. Thank you very much.

**ROD DIRIDON:**

Quickly, let me inform you all that Secretary Chertoff is here, he's being debriefed after his morning testimony before the Committee, so there's time for Polly. Norm is not here yet, so we're going to wait until Secretary Mineta arrives and that ought to give Polly 15 minutes to make her presentation.

**GREG HULL:**

Well, thank you very much, Robert. Obviously I think that you'll agree with me that Robert's got a very daunting task over at the TSA and for those of you making your way to the door, I wouldn't do that, because Polly is up next, and she's armed and dangerous. One of the things that has become very critical within the Industry and the TSA is the partnership that Robert talked about. We're still working very hard to form these partnerships though technology and other

areas, such as training. Many of you know our next speaker, Chief Polly Hanson. Polly has been a strong force in advancing our industry's security needs, for WMATA (Washington Metropolitan Area Transit Authority) and all of our industry. She has spent a lot of time on the Hill and a lot of time with the various committee members on the Hill to talk about our needs. Chief Hanson is the first woman to lead the Washington Area Metro Transit Police Department and is only the second woman to hold such a position at a major transit agency. She leads a department of 400 sworn police officers and 130 non-sworn personnel in three states, and she oversees an operating budget of \$44 million for the purpose of safeguarding more than one million Metrobus and Metrorail customers in a patrol area that covers more than 1500 square miles. Chief Hanson is a graduate of the FBI National Academy and the FBI Law Enforcement Executive Development Seminar. She also holds a Master of Science degree in applied behavioral science from Johns Hopkins and a Bachelor of Arts degree in radio, television, and film, from the Annenberg School of Communications at Temple University. Chief Hanson has been a member of numerous project panels for the Transportation Research Board of the National Research Council and she serves on the law enforcement executive team that plans special events in the Washington, D.C., area. Please join me in welcoming Chief Polly Hanson.

**POLLY HANSON:**

Greg knows how much I love baseball, so he gave me the pleasure of being the cleanup batter. He told me I didn't have to hit a run, just advance the runners, so I will proceed by wrapping up the inning by trying to put together what we've heard up until now.

So far what you've heard is that transit properties are using a layered approach to allocating resources for security, which in some properties includes screening passengers and in others does not. In developing a program to screen passengers, we now have the ability to take advantage of the benchmarks and the best practices established by our colleagues in New Jersey, New York and Boston, and we have the opportunity to review the lawsuits and the case law. We also need to consider ADA (Americans with Disabilities Act) and demographic impacts for our customer communication efforts. To do this we can use research such as the studies by the TRB (Transportation Research Board), Ron Frazier, the Mineta Institute. We also need to be seeking the support of our customers through public campaigns, Web sites, and outreach efforts in the media. I noticed that Lena Son from the *Washington Post* is here. The use of special events,

national security events or threats are sometimes opportunities to launch or implement passenger screening programs, but these programs need to be strictly supervised. They need to involve highly trained personnel that can set up the screening quickly. And then be able to use statistically random, selective or consent searches that may or may not involve canines, special screening technology, counter surveillance or hand searches. This is something that some people are doing, and that almost everybody's considered.

Many in the room believe that we are being complacent, because we're continuing to move further and further away from September 11. We believe that this complacency is the accomplice to terrorism. Mr. Millar said that protecting our nation is protecting our future. I would suggest that what we're all trying to do is protect our transit systems which in turn protects our nation and protects our future. I think now we're ready to conclude, and you said we were going to take questions later, and so back to Greg Hull.

**GREG HULL:**

We can always count on Polly to be very succinct and thank you for doing that wrap-up. Obviously we've had a lot of information provided to you through this panel. As Rod mentioned earlier, we're not going to take questions at this point, because we do need to move along with lunch and our luncheon speaker who will be introduced shortly. What I would ask you to do over the lunch period is to think about the questions you would like to pose to the folks here on the panel to raise after lunch and after our keynote speakers. There's a lot that they can share with you yet through your questions, but before we turn it over, let's show our appreciation to our panel members.

**MORT DOWNEY:**

To introduce the introducer is always an important role in these events. I had been told earlier that the next speaker wasn't going to be here and that I would have to fill both ends of that job, however, I'm very pleased to see that Norm Mineta is here on the screen. I will remind you that he was Mayor of San Jose, and was a member of Congress for many years. I got to know him when I joined the staff and he joined as a member at the same time. I won't say what year that was, but I will say that it was awhile ago. Norm went on to become Chairman of the House Public Works and Transportation Committee and was involved in many different pieces of legislation over the years, both in aviation and surface transportation. He left for a period of time

to go into the private sector, but the public sector always seems to call him back. He served as Secretary of Commerce in the Clinton administration and later as the Secretary of Transportation in the George W. Bush administration. We all know what a tremendous job he did in that regard, not just on September 11, although that was clearly one of the most visible parts of his tenure, but building, renewing and remaking America's transportation system. We've all lived well on the programs and the ideas and the energy that he has brought to the transportation world and it's terrific to have him here today to speak with us.

**NORMAN MINETA:**

Thank you very much, Mort, I'm actually in London, as you can tell. This afternoon I'm heading to San Diego. It gives me a great deal of pride to be able to be here today. First, because I now have the opportunity to thank all of you for taking the time from your own very busy schedules to be part of this security symposium, and second, because it gives me the opportunity to introduce my very good friend Michael Chertoff. I first met Mike when he was the Assistant Attorney General in the early part of the Bush administration, and then he left to become a federal district judge in New Jersey. Then I remember there was this announcement about Judge Chertoff coming down to become the secretary of DHS. I called Mike and said, "You're giving up a life-tenure district judge position to come back and jump into the fire?"

The Department of Transportation is involved with safety and the Department of Homeland Security with security, and safety and security are inextricably linked together, so we worked together on a daily basis, so whether it was under Secretary Ridge or Under Secretary Chertoff there were Memorandums of Agreement, Memorandums of Cooperation, and Memorandums of Understanding. Those are all on paper, and the value of that kind of linkage between safety and security comes from the ability to work together, and I never had a better co-equal in being able to work at the capitol level than Mike Chertoff. He is bright, he and his wife Merrill are good friends of my wife, Deni, and me, and we enjoy their friendship. This country has been well served in every respect, whether Mike has been in the judicial branch, in the private sector, or in the executive branch. With that, it gives me a great deal of honor to have the opportunity to introduce Secretary Michael Chertoff to all of you today.

**MICHAEL CHERTOFF:**

It's really a great pleasure to be here, be here with Norm. He was a terrific cabinet colleague, not only by standing and running his own department, but because of the level-headed advice he gave to the president and to his colleagues. He is a tremendous public servant who's continuing to serve the country in a lot of different ways. I also just want to recognize Brian Michael Jenkins who's written a very important paper. I think we met out in California sometime last year, and he always writes very provocative and interesting things about the threat of terror. I also have to say that I did get one legacy from Norm Mineta that I still have, and that's Michael Jackson, my deputy, who still occasionally veers off in the direction of the Department of Transportation. Sometimes I have to remind him, he doesn't work there. He has a deep reservoir of knowledge of the transportation sector along with his expertise in Homeland Security, and that's been an element of strength to the department. Finally, I want to commend MTI's work in transportation security. Long before 9/11 MTI had focused on the area of transportation as a potential target for terrorism, and I think it's important to continue to talk about it and speak publicly about the very important issues involved in transportation security.

If you look at some of the activities since September 11, 2001, which involved either threatened terrorist plots or executed terrorist plots, virtually all of them involve transportation. Public transportation is a target partly for psychological reasons and partly for strategic reasons. Al-Qaeda and its affiliates continue to see transportation as a symbol of the west and as an important element of the economic infrastructure. We have the attempted airline plot of August of last year, we had the two London subway plots, one of which was successful, one of which was not successful, we had the Madrid plot, and all of these focused on transportation. Now we all know mass transit is vulnerable, particularly rail transit. In aviation, where even though you have tens of millions of travelers every year, they are only funneling through a small number of portals, and they're operating in a highly structured system. Public transportation is completely different.

I have spent a lot of time on the New York subway. Flow, speed and efficiency are the cornerstones of the system, yet because of these factors and because of the open architecture of the system, the issue of security poses a dilemma. The dilemma is that the very thing that makes mass transit work is its fluidity. But its many open portals and its very fluid architecture are also the things that make mass transit and rail transit attractive to terrorists. So we're confronted with the fact that the very strength and foundation of our mass rail transit system is in fact its greatest vulnerability to terrorism, and that has to be the starting point for any rational discussion. How

do you strengthen passenger rail security after September 11? How do we cut that risk down without seriously compromising the entire system?

The first thing we have to do is recognize the terrorists themselves. If we can take them out or identify them or incapacitate them, that is the first and best level of defense we have against their mounting an attack on our transportation system. For that reason, we work with others around the globe to disrupt terrorism at its source and we have customs and border protection officials who create a line of defense at the border. If we can get the right amount of information and properly analyze it, identifying and neutralizing terrorists is the most effective means of stopping people who want to come in from outside, before they can get into our own country. As for the possibility of homegrown terrorism, it is the responsibility of federal, state, and local law enforcement inside the country to identify and disrupt it by gathering good intelligence. If you go back to the 1990s, you know there was a plot that a blind sheik was trying to execute. He planned on detonating bombs on bridges and tunnels in New York. So, clearly, if we can nab them and stop them before they get started, that is the best way to prevent an attack on our transportation system.

However, we have to recognize that we're not always going to be able to pick them off before they try to enter the system. So the challenge becomes, how do we screen for terrorists who are carrying bombs or similar weapons? In the context of today's world, we have to reject two extremes in the way we could approach screening in mass transit and rail transit. On one side, we have the extreme where we try to screen everybody, as we do at airports. The other extreme is that we don't search anybody. Everybody comes and goes as they please and we're just going to hope that the other measures we have in place protect the subway.

First, let's assume we try to screen everybody. Well, that would certainly make it harder and less attractive for terrorists to target the transportation system and our mass transit system. However, how many people are there during rush hour in Washington or New York who use the mass transit system and what would the lines be like if everybody went through a magnetometer? How quickly would they find other ways of getting to where they need to go? Or, worse yet, would they stop using public transit and move out of the cities? Thus, it becomes pretty obvious that screening everybody is simply not a realistic option if we're going to protect the system.

On the other hand, while it would be very time-efficient to not do any screening, it creates a vulnerability which is an invitation to a terrorist. So if we're going to use screening as one of the layers of protection for our rail system we have to be balanced in the middle. We have to avoid screening everybody, but we cannot afford to not screen anyone.

What we have to do is screen some people, though we cannot hope to do all. What we typically do now is we screen them in a random fashion because that way we get some coverage but we are able to modulate the frequency so that it doesn't inherently disrupt the architecture and flow of the system. Now I'm going to tell you that there's no doubt in my mind that random screening, including random screening with dogs, is better than no screening. It is a deterrent against terrorism and even a partial chance of being caught does deter terrorists who fear failure as a major element of their planning process. It decreases the vulnerability of rail transportation in a way that still doesn't fundamentally undermine the way that the system works.

However, is this the best we can do—random screening? We need to recognize that in the real world, it's difficult to do truly random screening. If we tell screeners to screen randomly without any further instructions or guidance, they're going to try to do it, but inevitably other criteria are going to enter into the picture. They are going to need to sort through the vast majority of people who come through the port or through the subway and they're going to have to decide who they want to focus on. Some of the criteria that they use, particularly those based on personal experience, might turn out to be pretty good criteria. For example, they might screen people because they look panicky, or because there's something about their behavior that raises suspicion. That would probably be a legitimate way to begin to narrow down the set of people that you're screening. It all depends on whether the individual screener has acquired the knowledge and has the ability to recognize potential threats. It's also possible, though, that screeners might rely on other tests that we would not want to have them rely upon, such as racial or gender profiling, or something that we would not consider to be appropriate. Even if you were totally arbitrary in screening, and you had a random number generator, it's not clear to me that random screening is the best we can do.

So how do we improve screening? Well, I think what we do is something similar to what Professor Jenkins's white paper talked about today. I like to call it informed random screening. Random screening that is informed by training and actionable indicators that are appropriate in

managing and identifying risk. Now I should say that at the borders when people come in by air, we use informed screening, and we're able to use it because sometimes we get a certain amount of information about the identity and the behavior of people who come into the country by air even before they land based on some of the data that we acquire from the passenger name records held by the airlines, as well as passport data. This gives us a very intelligence-driven capability to make intelligent screening choices at the border; but it's quite obvious we can't get advanced notification for a subway, so we have to use a different model to identify the kind of comments and criteria that would allow us to do informed random screening.

I'd like to suggest what some of these might be: physical behavior or appearance, and by that I mean if it is a hot day and you're wearing an overcoat or if you have something bulky in your clothing. If we can train our screeners to look at those kinds of criteria, that's a good way to start informed screening. Teaching people about behavior, as we're doing at TSA, can also be very useful because it alerts them of individuated characteristics that would suggest that they should take a closer look. Another way to make informed random screening decisions is to focus on proximity to a target of high value: to put more of your screening in those stations or those areas where there's a symbolic target. If there's a higher risk, someone may be more likely to try to drop a bomb there. Time and route of travel should also be considered. There may be some routes which are centrally located and where the damage that could be done by a bomb would be much greater. You might want to step up your screening there to take account of the fact that there's an increased consequence of an attack. Look at putting extra effort into screening near tunnels, especially those underwater. I think in addition to that, there are some new technologies we're working on to aid our screeners and police. Some of it involves explosive detection techniques that work on a standoff basis, and we're testing some of those at the Port Authority of New York and New Jersey. I've also heard some reviews about potentially using hostile-intent systems in conjunction with surveillance CCTV cameras that would help us detect what we could describe as anomalous behavior. Underlying all of what I've said, random screening can be informed by either technologically or techniques of narrowing the field of suspicion.

This is the philosophy that's needs to underlie all kinds of public transportation, whether it's rail transportation, air transportation or another kind of infrastructure protection: We can never totally eliminate risk, but we can help manage risk. We need to make decisions based on understanding of a threat, on a determination of vulnerability, and, finally, on an appreciation of

the consequences of an attack if it were successful. Balancing all these elements and then applying a cost-effective approach to what activities we undertake has got to underlie not only what I'm talking about with respect to screening in mass transit, but more generally what we do to secure our transportation system and all of our systems across the board. That's the approach we have increasingly implemented at the DHS: risk management as a philosophy of decision making.

Since September 11, we have provided over \$20 billion in awards to state and local governments for programs and equipment to help manage risk. Each year, we are refining the tools and the approach we take to better focus on the higher-risk areas as a way of driving grant funding and grant management with respect to mass transit and rail transit. This year alone, the nation's eight largest mass transit rail systems have been awarded a \$103 million in security grant assistance. When further awards are made later this year, the total will rise to \$278 million. Through our transit security grant program, we've provided nearly \$392 million to-date, to 60 of the country's rail, mass transit, ferry, and intra-city bus systems in 25 states and in Washington DC. The President's budget request for fiscal year '08 will push the total to \$564 million, and states and localities are encouraged to tap into other homeland security grant programs and urban area security initiative funds for rail security projects and initiatives.

Now, even with this very substantial amount of money, plus the in-kind assistance we give in terms of things like biohazard detection equipment and research and development I often hear that we're not spending nearly as much on surface transportation as we do on air transportation. I do think this requires at least a moment of reflection. While it is true that there's a big difference, that's also because there are two big differences between the aviation system and the mass transit system. The first is that we actually employ the screeners that do our aviation screening at our airports, as well as the air marshals who are on the airplanes, and the federal security directors. And I have not yet encountered a city transit system or a state transit system that has requested to have us federalize the police force for that system. You can't really compare what we do for aviation to mass transit because 60 to 65 percent of the money we spend on aviation is personnel costs, and we're not doing personnel for state and local governments in mass transit because state and local governments are doing it. It's also true that we are heavily equipment-dependent, and a great deal of our expense in aviation is for putting in explosive detection equipment in portals at all of our airports. Again, that's not the architecture I've heard anybody say they want to see at

our subway stations and our commuter rail stations around the country, so this is a mismatch when you compare the two simply in terms of dollars. The systems are very different, they're both very important, but the architecture of mass transit and the fact that state and local personnel have the responsibility for doing the patrolling and the security in mass transit means we have two different funding models and two different operational models. Nevertheless, I am aware that rail transit is a vulnerable target. Therefore, I'm as determined as anyone in this room to ensure that it gets the investments it needs to protect itself.

Ground transportation needs cutting edge research and development, as well as funding for things like closed circuit TVs, additional canine teams, and the benefit of some of the intelligence that airline security receives regularly. We should continue to talk about this, and the DHS is always open to hearing suggestions, and discussing how we can improve ourselves. We're going to continue to work to make sure that grant monies are spent wisely, but, more important, we're going to work to ensure that all funds are integrated with an overall strategic approach to managing risks. Only if we adhere to that philosophy can we be sure that we actually don't give the enemy the victory of destroying our way of life. Thank you very much for your attentiveness, I look forward to continuing to work with you on these issues, and now I'll take a few questions.

**MORT DOWNEY:**

Those of you who were panelists this morning, do any of you have questions for the secretary?

**CHRIS PEOPLES:**

Mr. Secretary, I'm a little bit of an anomaly here because I represent a bus-only district. Could you say a few words about what you're doing aside from providing us some money for cameras? What do you think is possible in our major urban bus systems?

**SECRETARY CHERTOFF:**

Busses are even tougher than subways because of the open architecture. You will need to improve intelligence information, training, bus security in terms of bus depots, but I don't think anybody's come up with a way you can screen people getting on and off a bus. I think we also need to review our response capability, there's tendency to assume that the whole name of the game is prevention and hardening, but in the case of some systems, and particularly a system

that's very open like the busses, a lot of what may be important is the capability to mitigate and minimize the damage: having highly trained response teams which are able to rapidly respond to any incident is important. Overall improvement of bus design could also be investigated: things that create greater resistance to projectiles or explosives. Those are areas where I think we can work and productively be partners for bus systems in terms of increasing your security.

**POLLY HANSON:**

Hi, I'm Polly Hanson of the Chief of the Transit Police here in Washington, D.C., You alluded to the difference between mass transit and aviation when you talk about the staffing and who funds that staffing. I recently had the opportunity to participate in a base inspection done by federal rail inspectors, and I know that there's currently a proposal that suggests that there could be 500 additional inspectors, and I wonder if maybe the industry would prefer to see those funds go to transit security grants so that some of the other things that we need to do that are either identified through base or other vulnerability assessments are done instead.

**SECRETARY CHERTOFF:**

The question of where you allocate money is a subject of hot debate. We have responsibility and also to provide a service in terms of advice. You could say, well, why don't you save your advice and just give us the money? You could take the position that the federal government ought to simply get out of the business of mass transit, make it a local function, give some grants, and then say it's entirely a local responsibility. We'll give you a little extra money and then you take care of it. But, then, of course, if something happens, are people going to come to the federal government and ask why we didn't do something about it? One thing I've learned in the years I've been in government is that you want to make sure you have well-aligned responsibility, capability and accountability. The public expects that, with respect to acts of terror—particularly international terror—that it is ultimately the federal government's responsibility to provide safety. We have to have the ability to use our assets to make sure that we are reviewing what's going on and ensuring that there is an adequate level of capability. That doesn't mean we want to take over or undermine the local systems, I think that would be going in the wrong direction, but it does mean that we are going to spend some money on our assets to make sure that we are capable of monitoring what's going on.

**DOUG DELEAVER:**

Mr. Secretary, Doug DeLeaver. I'm the Chief of Transit Police in Maryland. When we get our grants, they come in at the state level. By the time they filter down; they have been divided and chopped up. We have twenty-three counties in addition to the state organization. So, is there some way, when the grant comes down, that it be designated solely for the state, and not for all the different counties? At the state level we have the Marc trains, busses, and subways, light rail, etc., whereas the county only has a merry-go-round bus]. We tend to get left out of the loop when it gets down to the state level, because the government chops up grants so as to ensure that everybody gets something, and we're left out.

**SECRETARY CHERTOFF:**

The way we do our grants is that we have transit grants that have to be focused only on transit programs. Here's a dilemma in which we find ourselves: when we're meeting with city officials, they'd like to give the money to the cities, county officials want it to the counties, state officials want it to the state, and each and every state is different. In Texas for example, the state government is comparatively weak and the county government is really strong. In New Jersey the reverse is true, where there is a very powerful state government. We can't possibly figure out how to make the system fit every one of the 50 state systems, knowing when we should give it to the county, when to the city or when directly to the state. We have to rely on the basic building block of federalism: the state government. When we do urban grants, which are the exception, we drive for regionalization, but at the end of the day, we can't be telling governors, that we're going to bypass them. The last thing I want to see happen is for us to get caught in a political fight between the state and the county, because we have no business being there. Although I'm very sympathetic to these issues, we're certainly not looking to have a lot of money stay up as overhead. I think at the end of the day, from our standpoint, we need to have only one belly button through which we can funnel these grants.

**MIKE CONNORS (BOOZ ALLEN):**

Secretary Chertoff, I wonder if you could comment on the state of fusion, of giving intelligence to the transit police departments.

**SECRETARY CHERTOFF:**

We are doing this largely on a state level, although in some cases we're doing it at a city level in some very big cities. We are building out fusion centers that will be partly regional if not statewide. And it's expected that within a given center there will be representation from the appropriate transportation security authorities, so that they can receive the benefit of federal information. In addition they can help feed in information, because you are intelligence collectors as well as intelligence consumers, and, therefore, again, the fusion process is a way of trying to have a fewer number of connectors that have to be met, in order to aide in the flow the information. These centers will be constructed as opposed to everybody conducting their own ad hoc deals where so and so calls his friend up and passes the information, but he doesn't get diffused in a systematic or orderly way that can be tracked.

**MORT DOWNEY:**

Thank you, Mr. Secretary. It is very encouraging to hear the level of sophistication that you're speaking of.

**ROD DIRIDON:**

We'll now begin the Q & A portion of the program.

**MORT DOWNEY:**

Robert Jamison has to get back to a meeting at the department, but we certainly want to thank him for being with us this morning. We now have some time to reflect on and take questions on this morning's discussion. Let me start it off by asking each of the panelists to reflect on what we heard from Secretary Chertoff, and how you think that establishes the working relationship that we'll need to have to provide security and mobility. Let me pass it on to Polly first and run on down the line.

**POLLY HANSON:**

I am an advocate for transit security, being the Chief of the second largest rail system and, depending on what day of the week it is, the fourth or fifth largest bus property. With all due respect to the secretary, I understand what he's saying, but I think most of us in transit policing that have had the opportunity to participate in funds, it's a hard battle to convince your local colleagues as to why transit is more important than their particular infrastructure. Certainly at the state level, for many transit properties, transit grants are the only opportunity they have for

funding because many of us are facing state budget shortfalls. We all know that mass transit is not something that makes money, and that we have responsibilities from the FTA to designate percentages of our federal funding towards security. In the case of WMATA (Washington Metropolitan Area Transit Authority) our budget is \$50 million in addition to the \$50 million for the budget of the police department. In that budget there are “x” percentages of money going towards infrastructure security in the way of new fences, updating to intrusion alarms, capital projects that transit properties do, and assessments that we participated in.

There have been a number of assessments that we’ve had done in looking for access to federal dollars. And we are currently implementing the recommendations from prior assessments, as well as new recommendations or mandates that are tied up with the guidelines for current or future security funding. Now there’s also the additional dimension of training, so there’s been a piling on of additional requirements—the tunnel security being the newest one—which are all very costly. So I think the people in this room that are directly responsible to our local and federal officials for protecting our systems and our customers have questions to ask, such as, are there better utilizations for funds? In the area of rail inspectors, do there need to be as many? Could some of that money then go back to transit security grants? Could the transit security grant program be more robust? There are a lot of people at different tiers competing for funds, and all of us trying to accomplish things that, depending on who did your assessment, a variety of federal agencies have instructed you to do. I think there is a sense of frustration, and I understand what the secretary is saying, but I do find a slight disconnect between his comment about airport and transit being different. If they’re talking about increasing the rail inspector program, I think those dollars could be diverted a little differently—to the transit properties themselves.

**DOUG DELEAVER:**

Now you’ve hit the home run, Polly. I agree with what Chief Hanson said, we are asked to do more, each year by the federal government, and they don’t give you any extra money. We have mandates for new things that we have to do and look at, and we have all this training that we have to do, all this equipment that we have to purchase, and things we need to change. We don’t get any more money for people, and state transit budgets always get cut, no matter what you do. You put in for a hundred cars, you get three. You put in for new equipment; when it comes to equipment for transit and law enforcement issues, the public looks to you to protect them, but

they'll complain quick if the cost goes up. So what Bill Millar said this morning: "We transport a lot of people, and we're just as important as airplanes." I went up there and looked at Chief Barbour's system, looked at New York's and Chief Hanson's. Between us we transport a lot of people—more than airplanes—but they don't give us a comparable amount of money.

**MORT DOWNEY:**

Bruce, the Secretary's comments about screening, how did that fit with your research and thinking? And Brian?

**BRUCE BUTTERWORTH:**

Actually they seemed very compatible, and I don't have much to add, really. They're different terminologies, but essentially it's pretty much what we're recommending in the report. It might be a good idea for someone to take a good look at what happens in an attack on a mass transit system in terms of the economic effects on that city—not just in terms of the immediate loss of business and labor productivity, but what happens if you lose tourist income. That would start to change the risk/cost-benefit analysis, and it might affect the cost-benefit analysis between aviation and mass transit. I'm not sure people appreciate just how much economic impact a successful attack on a mass transit system could cause.

**RON FRAZIER:**

I had a couple of notes that I made from the Secretary's comments. The first has to do with terminology more than anything else. From a legal perspective I made a note about "informed random screening versus selective screening." I'm not quite sure how that plays out, but, obviously, from the standpoint of legal ramifications, selective can be a kind of a funny word. We have to try to figure it out and work it out. I think it means the same thing, and I suspect that we can try to figure out the best way to phrase these countermeasures. The second comment that I specifically heard the secretary mention concerned the concept of location, as in determining which targets are high-value. What I didn't hear him say was something we have to think about in terms of planning from a legal perspective, things like setting up screening at a station when it's in an ethnic neighborhood. Those sorts of things are going to be just the opposite of what we need to do here. For example, if there is a community where there are mosques and you decide to go there and set up all your screening at that station, you're going to raise unnecessary issues.

Finally, the Secretary said that the only way to eliminate risk is to eliminate the risky activity, but that what we actually are doing instead is managing risk. I thought that was particularly true as it relates to in the legal sense as well. The starting point should be: “How likely are terrorists to attack the system?” and “If the system were attacked, what are the most vulnerable assets, and the most critical to operations?” and “How could the agency best protect those assets?” These are the areas which help you determine how reasonable it is to screen in a certain area and helps determine your operational considerations.

**MORT DOWNEY:**

Brian, what was your reaction to the Secretary’s assessment of the vulnerability of our transit system?

**BRIAN MICHAEL JENKINS:**

It is vulnerable; the problem that we have in protecting public places is twofold. One, it is difficult and costly to protect public places; second, in protecting public places we have to be very mindful of the net security that we obtain. Our goal as a society can only realistically be to displace the risk from one set of targets to another, where that second set of targets is clearly less lucrative in terms of casualties. I regularly hear people on the Hill talking about the need to protect shopping malls or something like that against the random bomber. In this case, I’m mindful of the fact that this would involve trying to protect the tens of thousands of shopping centers across the country. If our presumption was that there is a single, determined terrorist bomber, what in fact we would achieve as a net benefit is that we’d merely force the bomber to drive another two blocks to a hotel lobby, a supermarket, a theater, etc., so we do have to be mindful.

There has been voiced a justifiable complaint that all of you with security responsibilities confront about the issue of federal mandates without federal funds to back those up. Given that local governments are so strapped for funds, I would like to give a cautionary note for when you are looking for additional federal funding: The people who provide the money, they get to make the rules. You have to be careful that we don’t end up in a situation where the best practices that are offered and become goals don’t turn out to be regulations. A large flow of federal funding coming down to these local operations is inevitably going to come with a set of regulations. No

one starts off hoping to create a federal regulatory system, but you can end up over a period of years creating one anyway. This just comes across a consequence of the flow of funds.

Some of you mentioned in the panel that some of the operators were doing selective screening, and some are not. The report that Bruce and I authored is not advocating that all of you or any of you implement a selective screening process. On the contrary, what we would propose is that you think about how you would do it, in advance of an event or in reaction to specific intelligence or in the face of any specific threat. It could be a major incident in the U.S., which is going to require all of the other operators to think about what they can do, either to prevent another attack—a copycat—to merely to reassure their riders, or in reaction to an incident elsewhere in the world. I mean the reason Boston went to screening was because of a national political convention, so we are not saying that everyone ought to have selective screening, but rather there ought to be careful thought and planning as to how you would do it. So that when you are required by circumstances to do it, you have your plans in place.

**MORT DOWNEY:**

Also, if you're thinking about a new facility or rebuilding a facility, designing in that capability to do it if you need it would be a big plus.

**BRIAN MICHAEL JENKINS:**

Anytime we have an opportunity to renovate, rebuild or build a new a station, etc., security ought to be a criterion from the drawing board. This planning could even possibly include the creation of a red team, separate from the architectural teams that will look at augmenting security and screening. Those who have security responsibilities slide into the trap of viewing the world exclusively from the perspective of someone with a security responsibility, but there are non-security solutions to security problems. When we build things new, as we are in some parts of the country, refurbishing decaying transportation infrastructure, we have the opportunity to make it more robust, to build in redundancy, to make it more resilient, to facilitate rapid recovery, and to design in the basis for future security technology and procedures that might come into being. By keeping in mind future technologies, future procedures, at the design stage, we can more quickly and effectively build them in.

**BILL MILLAR:**

Maybe I ought to be at the end of the panel here. Those of you, who know me, know that I just showed an incredible amount restraint as you were all throwing a bunch of red herrings. To make a distinction as to who employs the person as to the need for funding for personnel costs, in my humble opinion, is absurd. To suggest that we at the federal level don't know how to deal with more than fifty grantees at a time is not only absurd, it denies the great work that this gentleman and his department did and that his department continues to do every day. We have suggested for five years to DHS and its predecessors, let the FTA, which has already the relationships for the grants, go ahead and pass the money through. It is not, as they say, rocket science. To have people come out and inspect things that you know are not getting done because you haven't funded them is an enormous waste of effort and resources; it's just more people-watching-people. We testified last week in front of the Congress on just that point, because no one is telling me that the VIPER teams have been useful or that the VIPER teams have known what they are doing when they get on their property. Now, that may be an unfair criticism, as it's early on, and maybe some day they will become useful and will know what they're doing.

I'll tell you a story. One of our large bus system operators tried to take some of the money that has been provided and purchase security cameras for their bus. That seemed like a logical basic piece of infrastructure they should have, but he got back a lengthy, written explanation as to why security cameras cannot be funded, or that if they are funded, it will depend on the angle of deployment of the security camera. If the angle is set so that the majority of what it looks at is outside the bus, it is not permitted with DHS funds; however if the angle were such that it would be primarily in the bus, depending upon where in the bus, it is possible that that it could be viable. I don't know about you, but when I'm paying my federal income tax, I don't really want them to make that distinction, because apparently if my dollar goes to the Department of Transportation, I can look outside the bus, but if my dollar goes to DHS, I can only look inside the bus.

Doug's point about what happens when it all gets filtered down is a really good point. We need to stand in a unified way and speak to the department and tell them what we want to have, but you've got to listen and you've got to learn to make improvements in things.

**MORT DOWNEY:**

Thank you, Bill. Questions for the panelists—yes, sir?

**GORDON NEVUS:**

Hi, I'm Gordon Nevus of The Nevus Group. I was following Bill's speech, and I wonder if the panel might comment on how we mostly talked about big systems, mass transit systems, in the light of the fact that the majority of transit systems in this country are 200 busses or fewer. It's the small systems that struggle every day just to get funds together so they can buy vehicles, with basically no money for screening or security, and I wonder if the panel might comment on how they think that some of these DHS funds from wherever should flow down to those small systems. Also, what they need to do to help secure those systems.

**POLLY HANSON:**

Good luck. Certainly you heard the secretary, and I know that Robert talks about regionalism and recognizes that some of the smaller systems feed into larger systems. People really have to understand the impact and the consequences if something were to disrupt transit. For example, during Hurricane Isabel in Washington, D.C., we made the decision to close our system and every local jurisdiction in this region closed because we closed. That proves that our relationships with the regional transportation agencies are important. So, demonstrating to your local municipalities the impact of the lack of transit, and proving their value, will help provide you an opportunity to access those funds. Some of what Brian Michael was talking about was the type of things you could build in your bus shelters, at your bus turnarounds and at your major facilities. You're multi-modal with other types of transit or other transit properties, and certainly those relationships can help you get the big person in this region to recognize your importance. So, I think it's proving your value to the region so that they are kind enough to free up some of the scarce funds that you typically do not get. Certainly, as you go forward building new facilities or purchasing new busses, go ahead and make sure that you're purchasing busses with cameras or that you're working on target hardening or crime prevention through environmental design in your new facilities.

**MORT DOWNEY:**

Let me ask Bruce about technology: with respect to the smaller systems, what is out there that may bring new capabilities?

**BRUCE BUTTERWORTH:**

That one I can't tackle totally. I suppose some of the standoff technology when applied at smaller throughputs could be of use. It all depends on what kinds of lines are coming into these. You're talking about bus systems, and I have to admit that we have not taken a good, hard look at them, and I am not aware of anyone that really has. It's an item that probably ought to be looked at. There was one issue that Deputy Undersecretary Jamison took with our paper—a small issue—and it was the question of how robust the current technologies are that could be applied to standoff detection. I think it may be a question of terminology. What we gave was a three-to-five-year forecast for full deployment. Now, if you actually ask me the question of how long it would take to get a couple of systems out at a couple of locations, that window starts to go down and gets closer. The comments we made on technology reflect my experience with technology in the aviation environment. Those of us that went through the EDS and trace detector campaigns know that a plan is one thing; getting it out there and getting it working properly is another. It can all be quite a big slog. What we're trying to do is put a dose of realism into the environment, and one wants to make sure that when people talk about technology, they don't use it—consciously or subconsciously—as the reason not to provide more available assistance now.

**MORT DOWNEY:**

And what do you use in the meantime?

**BRUCE BUTTERWORTH:**

And what do you do in the meantime, with that five-year window? Well, what you are not going to do is wait until the technology shows up.

**BILL MILLAR:**

Our friends at the FTA tell us there are over 6000 separate providers of public and community transportation. The top 30 systems carry 70 percent of all ridership nationwide. What we hear from smaller systems is that, first, they believe that they should be able to do very limited, cursory threat analysis. They want to be able to speak with members of their community and have the resources to see if they have a problem. Secondly, they would like training available to them and to their employees even if it is a lower level of training. They rarely request anything resembling that of the major transit agencies but they do request the basic things they need to

help mitigate risk and be able to assess what's going on in their systems. So, we have taken the stand that there is a basic level where we all ought to be. We would certainly endorse Polly's comments about how it doesn't matter how many busses your major system has, the threat to the system can remain the same. You probably ought to treat different systems at different levels, but they all need some level of security for mitigating risk.

Quickly, one anecdote: three or four years ago, many of us participated in the development of a list of 20 things that transit systems should do. It was time for training and review of one of our small members in Iowa; this system was about a forty-bus system, something like that. The FTA comes out every three years to go through all 20 things, and they hadn't done number 19. So, when we brought it to their attention, it was changed. But the operator turns to me and says that right next to where he has his bus operation, is a huge Tiger Disk ammonia plant which has no fence around it, no security at all. He said as he was going through this checklist he was just scratching his head, and wondering how his small system could be a higher priority than that dangerous factory.

**JERRY GOLTON:**

Bill, just one comment: one property represents only 25 percent of the mass transit riders in the United States, in the year, and they have a security program over \$1 billion. To put that in context, that is versus \$135 million for the whole United States.

**FRAN KERNEDEL:**

Hi, Fran Kenedel, FKA, Alexandria. I did want to commend the FTA with respect to how it deals with small properties and less exclusive properties. Four years ago, the FTA in collaboration with the DHS was very sensitive to the issue of providing public awareness and outreach for free to communities around the nation through their Transit Watch program that has been recently updated. I strongly recommend it, and it is available online on the VTA Web site under "safety and security." If your community does not have the money to create your own public awareness campaign, it's available in English and Spanish.

**KATRINA WALSH:**

I don't mean to be redundant, but if I seem a little bit nervous, it's because you're all very distinguished, but I heard you mention that the public is expecting you all to be their protector and you also mentioned that there's no more flag-waving out there.

Well, initially, in the Transit Watch we did a survey in 2003, and I recall speaking with people in New York and Boston who were saying that they are getting a great deal more reports from the public. We've got ten billion eyes and ears on our system, and it still seems like the public is not responding, and not reacting to the level that they really could. If you could just comment on that and discuss ways to generate public awareness, like American Red Cross CPR program where the public is very involved. How can transit do something like that?

**DOUG DELEAVER:**

A lot of transit properties have citizens' academies: you bring people in for seven weeks or so, and you teach them what you do, and they go back and they carry your message. Go out and talk to communities, I'm talking to a community tomorrow night—about 70 people. They want me to come out just to talk; they don't have any concerns, they just want to know what transit is doing. If you talk to people and if your employees help deliver your message, you are creating lines of communication. This morning, we were on a train, a young lady got on it, and the conductor knew her and was joking with her. We need to help people take ownership of their trains and buses. We had a project named Gibby when Derek Jones was at the MTA (Metropolitan Transit Authority), and I'm telling you drug addicts downtown were saying you're trying to take my bus from me, so it's ownership—you have to inject a sense of citizen ownership into everything you do. We did this project in Baltimore; 87 percent of the people in Baltimore do not own a car. They rely on public transportation.

**MORT DOWNEY:**

Polly, I hear you on the station PA every time I go through, is that getting through to people, are they listening?

**POLIY HANSON:**

Well, I would say that the difference between the American Red Cross and transit security, is people have heart attacks every day, and you know people that have heart attacks every day, and so it touches you in a way that, of course, the further we get away from September 11, and of

course, the events in London, it all begins to fade from our memory. So I think it is a matter of taking the everyday, regular events that happen in a transit system—service disruptions, person struck by a train, fires, criminal activity, and other events—that many of the emergency response activities would be very similar to those of a terrorist attack. We can use those occasions to encourage people to learn how to evacuate, to take it upon themselves to have a plan, to have another route, and certainly during the couple of times of year such as September, which is National Preparedness month, and October, which is Crime Prevention and Fire Prevention month, to use those as opportunities to create an open dialogue and to plan events and campaigns with your customers that talk about crime prevention and terrorism. You want your customers looking for suspicious activity and knowing who to call when they see something.

As for PSAs, Mort's probably real sick of hearing me, and I'm really sick of hearing me too, so we do try to change the messages that we broadcast because they become wallpaper and you have to come up with new campaigns. In working with the community you have an opportunity to bring your first responders in—the DOT, your Department of Public Works and others—into a setting where they recognize what their response needs to be. I think there were a number of opportunities to remind the public of their responsibilities to be prepared, to be ready, to have a plan, and it's just incumbent on us to use the everyday occurrences, like the Red Cross does with the heart attack, to remind our customers of those events and their responsibilities to work with us.

**KAREN KRAUSE:**

Hi, I'm Karen Krause from TRC Solutions. One of the questions I'm currently struggling with is the re-prioritization of the Fiscal Year '07 funding towards training. I hear this is something that is needed for the mass transit systems, but if you look at the DHS funding guidance, they want to reprogram it to specific categories; they want to allocate the funding immediately. The DHS wants to do mass training of thousands of workers within a year's time, and then they say there's going to be a list of certified vendors. I'd like to see what the list of certified vendors is, and to stress that many of the transit agencies already have their own successful programs in place. Can they use that money to pay their own instructors? Or do they have to get certified at these certified vendors? Lastly when I think about how to scope out and help the mass transit clients that we work with is, well, you say overhead and backfill is a knowledgeable category. Well, I

don't know if you've been involved in this through the FTA grants, but I've been involved with other DHS grants and training, securing reimbursement for the overhead and backfill of thousands of employees, and it's a whole new program in itself. You can hire somebody fulltime for a year just to do that. My view of how this program is coming down the pike, it reminds me of what was happening over at the TSA, where the DHS came and said, well, here's all this money for screening equipment, and they gave it all to them with just a letter, and they came back three years later, and now they said here's all the requirements you were supposed to comply with. And because some airports didn't comply properly from the ANF perspective, they got all these audits, and it looked bad. I wanted to ask Robert Jamison this question but he left: based on your experiences, what are the best practices for how to ramp up, distribute training, and also manage it effectively to meet grant requirements?

**POLLY HANSON:**

We are struggling with the same situation and many of us that have been doing this for a while will look back to the regulation, to requirements, such as having bomb containment trash cans, and this is a similar scenario where the cart comes before the horse. The training has not been developed and you're being told to go do it, or you're being told that you better hurry up and spend the money that you have been given when the training hasn't been designed. It's not because I adore Secretary Mineta, but I will say that I like Mr. Millar, because when some of this was in the FTA family, it was a little better thought-out. Their training programs were in conjunction with the transit properties and were thought-out and worked on and properly provided. "Warning Signs" was a great free resource for people in the way of training for bus drivers, where you could just put the DVD or the video in. There is a disconnect here with requiring you to provide training that has to be certified when the training hasn't been set up yet. The little bit of money you may get for the training, if you're trying to get all your people through training and you're going to use that for backfill overtime, you're not going to have the money to do it. So, everybody's thinking the same thoughts that you are, that you articulated so well, and I wish he had been here to hear the question, because it's one we all have.

**BRIAN MICHAEL JENKINS:**

Can I come back to the previous issue in terms of enlisting the public? I firmly believe that the public has to be enlisted in Homeland Security far more than they have been in the past. For

what they may bring in terms of additional information or enhancing our response capabilities they are invaluable. We have a lot of talent, and not all of it is in government. Being prepared, being enlisted, being educated, and becoming savvy about security, how it works, what its limitations are: these are antidotes to the terror that terrorists hope to create. We not only have to prevent terrorist incidents but we have to try to reduce the alarm that they create. We need to limit the extent we are consigned to the role of frightened passengers in this process, without any way to participate or know what's going on. That is really a way of cranking up anxiety, so I see it as a utility. One of the differences between, let's say, the Red Cross CPR program and things involved in security is that the more specific we can make the instructions to the people, whether it's the general public or the ridership, or whatever our target audience is, the better. I mean, I don't how many times we have heard the fact that it does become wallpaper. The "be vigilant" mantra has to go. "Be vigilant" has no operational utility whatsoever, and, so, if we're going to have people do something, this comes under the category of the PA announcements of don't park your car here—it just becomes noise after a while. Second, for those of you with transportation systems that have looked at the issue of enlisting the public, to really make this work, it has to go beyond the PA announcements, beyond the signage, and it really has to have a complete loop. The public has to be admonished, exhorted, encouraged, and persuaded to notify someone. The next step is the instructions of how to notify them, where to notify them, clearly marked phone boxes, or instructions, or whatever, which has to be part of it. We can't just tell them to report something suspicious and have the sentence end there. We need to tell them to whom, how, when, and where.

The third component is that there has to be visible response to public involvement. If people are reporting something suspicious, whether it's related to crime, potential terrorism, etc, and absolutely nothing happens, that destroys all incentives for participation. In London, where they've had a lot of experience in this over the years, in dealing with the IRA terrorist campaign, they admonished the public to be vigilant, gave them specific instructions, and there are clearly marked phone boxes and things of this sort where you report information. When you used these boxes a voice would come over the PA system—and this was sometimes unnerving—somebody would say, "You, you with the plaid shirt, step away from the bench," and you're looking around knowing somebody is watching. Then you have the arrival of uniformed police or staff that are going to look at the thing, the fact that an action brought a result, completed the communication

cycle and kept the people involved, made people feel that their efforts would be immediately responded to.

**MIKE DENEAN:**

I'm Mike Denean from DOT Volpe Center. We recently had the opportunity to help the Boston transit system put up a security system on their bus rapid transit tunnel, the Silver line from the airport, and one of the things we found after we implemented the system was that the bus operations people loved it, because they had visibility of every inch of that transit tunnel. I wondered if any of you could talk about whether we might get more out of our security technologies by coordinating more with the operations and safety folks in some of the other departments to make security measures tools of efficiency as well as a tool of security.

**POLLY HANSON:**

Well, what I would say is there's a link and that you have to have a blended approach to security. It goes back to what Brian was saying: if the operational employees can't respond properly when people ask them what to do, you have a serious problem. Part of the problem with transit properties is sometimes they do what they're supposed to do, but they don't communicate very well. The operational employee is the one that has the contact with the customer, so the people who sit inside that are responsible for safety and security and emergency management obviously have to cascade that throughout the organization and have it come from the operational personnel, because they themselves know best some of the things that we need to do.

**MORT DOWNEY:**

And I've had many conversations on this subject in the context of container movement. No system will ultimately be totally effective at keeping containers out of the country that you don't want in the country, but it will be far more effective if the system that's being used to track for security is the same system that's being used to track and improve and make the carriage of containers far more efficient. If your security system becomes the norm, if it becomes part of the business routine of the company in addition to adding security, I think when you come up with those dual-use, dual-application kinds of ideas, they're far more likely to be embraced and they're far more likely to be effective.

**ROD DIRIDON:**

I sense that we're reaching the end, so if I may conclude the afternoon with some comments. My first comment is to thank the panels from this morning, Brian and Bruce, as well as Greg, Doug, Ron, Polly, Robert, Mort, and our two secretaries, Mineta and Chertoff, especially because, technically, he's my boss. Also Bill, president of APTA, thank you not only for being here all day with us, but also for all the help APTA and Greg and his staff provided in organizing this event. I'd like to say thank you to Jim Swofford and Leslie Hamilton; Jim and Leslie are the ones who organized and ran this out of the Mineta Transportation Institute. We will be doing a summary of the proceedings, that's why we're asking for names, and the recording equipment will allow us to do a summary. The summary will go on the Web page of the Mineta Institute, and we'll give it to APTA, so you can have it on your Web page, too, or you can link to it. I'd like to add one more thing before saying good day to you, and that is, as you take this information out into the community, and you begin talking to transit riders, you need to remind them that although this is very sobering information, last year forty-four thousand people were killed on the highways just driving cars. There weren't a thousand people killed in all of those bombings over the last five years around the world, so, though we're certainly ready to fight the best way we can against terrorism, we should not discourage people from using mass transportation as the very safest way to move people to and from work and goods, to and from the marketplace. Remember to always add that when you're talking about these scary things, otherwise people get the idea that maybe I ought to drive my car, when driving cars is the least safe way to move around. So, thank you very much for being here, you are the ones that made this day successful, we appreciate you being the conduits of that information back to the people that will use it, and now have a very safe ride home, or better yet, use public transit.

# MTI FOUNDER

Hon. Norman Y. Mineta

## MTI BOARD OF TRUSTEES

Honorary Co-Chair  
**Hon. James Oberstar** \*\*  
Chair  
House Transportation and  
Infrastructure Committee  
House of Representatives  
Washington, DC

Honorary Co-Chair  
**Hon. John L. Mica** \*\*  
Ranking Member  
House Transportation and  
Infrastructure Committee  
House of Representatives  
Washington, DC

**David L. Turney** \*  
Chair/President/CEO  
Digital Recorders, Inc.  
Dallas, TX

**William W. Millar** ^  
Vice Chair/President  
American Public Transportation  
Association (APTA)  
Washington, DC

**Hon. Rod Diridon, Sr.** #  
Executive Director  
Mineta Transportation Institute  
San Jose, CA

**Ronald Barnes**  
General Manager  
Veolia Transportation/East  
Valley RPTA  
Mesa, AZ

**Rebecca Brewster**  
President/COO  
American Transportation  
Research Institute  
Smyrna, GA

**Donald H. Camph**  
President  
California Institute for  
Technology Exchange  
Los Angeles, CA

**Anne P. Canby**  
President  
Surface Transportation  
Policy Project  
Washington, DC

**Jane Chmielinski**  
President  
DMJM Harris  
New York, NY

**William Dorey**  
President/CEO  
Granite Construction, Inc.  
Watsonville, CA

**Mortimer Downey**  
Chairman  
PB Consult Inc.  
Washington, DC

**Nuria Fernandez**  
Commissioner  
City of Chicago,  
Department of Aviation  
Chicago, IL

**Steve Heminger**  
Executive Director  
Metropolitan Transportation  
Commission  
Oakland, CA

**Hon. John Horsley** #  
Executive Director  
American Association of State  
Highway & Transportation  
Officials (AASHTO)  
Washington, DC

**Will Kempton**  
Director  
California Department of  
Transportation  
Sacramento, CA

**Alex Kummant**  
President/CEO  
Amtrak  
Washington, DC

**Brian Macleod**  
Senior Vice President  
Gillig Corporation  
Hayward, CA

**Dr. Bruce Magid**  
Dean  
College of Business  
San José State University  
San José, CA

**Stephanie Pinson**  
President/COO  
Gilbert Tweed Associates, Inc.  
New York, NY

**Hans Rat**  
Secretary General  
Union Internationale des  
Transports Publics  
Bruxelles, Belgium

**Vickie Shaffer**  
General Manager  
Tri-State Transit Authority  
Huntington, WV

**Paul A. Toliver** #  
President  
New Age Industries  
Seattle, WA

**Michael S. Townes** #  
President/CEO  
Transportation District  
Commission of Hampton Roads  
Hampton, VA

**Edward Wytkind**  
President  
Transportation Trades  
Department, AFL-CIO  
Washington, DC

\*\* Honorary  
\* Chair  
^ Vice Chair  
# Past Chair

### Directors

**Hon. Rod Diridon, Sr.**  
Executive Director

**Hon. Trixie Johnson**  
Research Director

**Dr. Peter Haas**  
Education Director

**Leslee Hamilton**  
Communications Director

### Research Associates Policy Oversight Committee

**Dayana Salazar, Chair**  
Associate Professor and Chair,  
Dept. of Urban &  
Regional Planning  
San José State University

**Dr. Jan Botha**  
Professor, Dept. of Civil &  
Environmental Engineering  
San José State University

**Dr. Dongsung Kong**  
Associate Professor,  
Dept. of Political Science  
San José State University

**Dr. Jacqueline Snell**  
Professor and Chair, Marketing and  
Decision Science  
San José State University

**Diana Wu**  
Research Librarian  
Martin Luther King, Jr. Library  
San José State University



Funded by  
U.S. Department of  
Transportation and  
California Department  
of Transportation

