AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

SAFEGUARDING OUR NATION'S SURFACE TRANSPORTATION SYSTEMS AGAINST EVOLVING TERRORIST THREATS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION SECURITY

AND THE

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

SEPTEMBER 17, 2015

Serial No. 114–32

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PUBLISHING OFFICE

99–574 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
CANDICE S. MILLER, Michigan, *Vice Chair*
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
JOHN KATKO, New York
WILL HURD, Texas
EARL L. "BUDDY" CARTER, Georgia
MARK WALKER, North Carolina
BARRY LOUDERMILK, Georgia
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
NORMA J. TORRES, California

BRENDAN P. SHIELDS, *Staff Director*
JOAN V. O'HARA, *General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION SECURITY

JOHN KATKO, New York, *Chairman*

MIKE ROGERS, Alabama
EARL L. "BUDDY" CARTER, Georgia
MARK WALKER, North Carolina
JOHN RATCLIFFE, Texas
MICHAEL T. MCCAUL, Texas *(ex officio)*

KATHLEEN M. RICE, New York
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
BENNIE G. THOMPSON, Mississippi *(ex officio)*

KRISTA P. HARVEY, *Subcommittee Staff Director*
DENNIS TERRY, *Subcommittee Clerk*
VACANCY, *Minority Subcommittee Staff Director*

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

PETER T. KING, New York, *Chairman*

CANDICE S. MILLER, Michigan
LOU BARLETTA, Pennsylvania
JOHN KATKO, New York
WILL HURD, Texas
MICHAEL T. MCCAUL, Texas *(ex officio)*

BRIAN HIGGINS, New York
WILLIAM R. KEATING, Massachusetts
FILEMON VELA, Texas
BENNIE G. THOMPSON, Mississippi *(ex officio)*

MANDY BOWERS, *Subcommittee Staff Director*
DENNIS TERRY, *Subcommittee Clerk*
HOPE GOINS, *Minority Subcommittee Staff Director*

CONTENTS

Page

STATEMENTS

The Honorable John Katko, a Representative in Congress From the State of New York, and Chairman, Subcommittee on Transportation Security 1
The Honorable Kathleen M. Rice, a Representative in Congress From the State of New York, and Ranking Member, Subcommittee on Transportation Security:
Oral Statement 3
Prepared Statement 4
The Honorable Peter T. King, a Representative in Congress From the State of New York, and Chairman, Subcommittee on Counterterrorism and Intelligence 5
The Honorable Brian Higgins, a Representative in Congress From the State of New York, and Ranking Member, Subcommittee on Counterterrorism and Intelligence:
Oral Statement 6
Prepared Statement 7
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:
Prepared Statement 7

WITNESSES

Mr. Eddie Mayenschein, Assistant Administrator, Office of Security Policy and Industry Engagement, Transportation Security Administration, U.S. Department of Homeland Security:
Oral Statement 9
Prepared Statement 10
Ms. Jennifer Grover, Director, Transportation Security and Coast Guard Issues, Homeland Security and Justice Team, U.S. Government Accountability Office:
Oral Statement 14
Prepared Statement 15
Mr. Raymond Diaz, Director of Security, Metropolitan Transportation Authority (New York):
Oral Statement 23
Prepared Statement 25
Ms. Polly Hanson, Chief of Police, National Railroad Passenger Corporation (Amtrak):
Oral Statement 27
Prepared Statement 28

FOR THE RECORD

The Honorable John Katko, a Representative in Congress From the State of New York, and Chairman, Subcommittee on Transportation Security:
Letter 2

SAFEGUARDING OUR NATION'S SURFACE TRANSPORTATION SYSTEMS AGAINST EVOLVING TERRORIST THREATS

Thursday, September 17, 2015

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON TRANSPORTATION SECURITY,
JOINT WITH THE
SUBCOMMITTEE ON COUNTERTERRORISM AND
INTELLIGENCE,
WASHINGTON, DC.

The subcommittees met, pursuant to call, at 2:10 p.m., in Room 311, Cannon House Office Building, Hon. John Katko [Chairman of the Subcommittee on Transportation Security] presiding.

Present from the Subcommittee on Transportation Security: Representatives Katko, Rogers, Carter, Walker, Ratcliffe, Rice, Keating, and Payne.

Present from the Subcommittee on Counterterrorism and Intelligence: King, Hurd, Higgins, and Vega.

Also present: Representative Langevin.

Mr. KATKO. The Committee on Homeland Security, Subcommittees on Transportation Security and Counterterrorism and Intelligence, will come to order.

The subcommittees are meeting today to hear testimony on our ability to safeguard our Nation's surface transportation systems against evolving terrorist threats. I now recognize myself for an opening statement.

I would like to welcome everyone to today's hearing. I am pleased to be joined by fellow New York delegation Members Chairman Peter King, Ranking Member Kathleen Rice, and Ranking Member Brian Higgins to talk about a topic that is so vital to the State of New York.

Protecting our Nation's surface transportation systems requires full cooperation and participation at the Federal, State, local, and individual levels. An attack on any of our surface transportation systems not only disrupts the local economy and infrastructure, but would have a ripple effect to cities across our Nation. For example, in my own district in Syracuse, New York, we have a freight line that runs through our downtown area and provides critical economic benefit to the region.

The purpose of today's hearing is to assess our ability and readiness to detect and disrupt threats to our Nation's critical surface transportation systems.

Before we begin, I would like to express my pride and admiration for the four Americans that, through unrivaled acts of courage and bravery, were able to thwart a terrorist attack aboard a Paris-bound train on August 21, 2015. The heroic actions of these four men—Mark Moogalian, a teacher originally from Midlothian, Virginia; Anthony Sadler, a senior at Sacramento State University; Air Force Airman First Class Spencer Stone; and Oregon Army National Guard Specialist Alek Skarlatos—saved countless lives. They really represent the best of what America has to offer.

However, it is our responsibility to the American people to do all that we can to defend them against such heinous acts, and the American people should not be put in a position requiring them to defend their lives while riding a train, subway, or bus to vacation, commute to work, or simply to run an errand.

Since September 11, 2001, many people have come to think of a terrorist attack against the United States as one which is an elaborate scheme against a hardened target. Increasingly, however, the terrorists and their sympathizers are choosing soft targets. The Charlie Hebdo attack in Paris, the military recruiting centers attack in Chattanooga, and now the train attack in Paris are just a few of such examples.

I look forward to hearing from our witnesses today on their perspectives on the state of rail and mass transit security, to identify progress made since the terrorist attacks on September 11, and assess any remaining shortfalls and how to address them.

I ask unanimous consent to insert into the record a letter I sent to Administrator Neffenger from the Transportation Security Administration expressing my concern over the vulnerable state of security of our Nation's surface transportation systems. Without objection, it is so ordered.

[The information follows:]

SEPTEMBER 17, 2015.

The Honorable PETER NEFFENGER,
Administrator, Transportation Security Administration, U.S. Department of Homeland Security, 601 12th Street South, Arlington, Virginia 22202.

DEAR ADMINISTRATOR NEFFENGER: I write regarding the efforts and capabilities employed by the Transportation Security Administration (TSA) to secure the surface transportation sector in the United States. As the country faces growing and proliferating threats from lone-wolf terrorist actors, it is imperative that TSA responds to the threat landscape in an adaptive and proactive manner. Indicated by the recently-foiled terror attack on a Paris-bound passenger train in France, which was mitigated by brave U.S. service members, surface transportation security presents an entirely unique challenge in efforts to secure transportation.

As Chairman of the Subcommittee on Transportation Security, I am concerned that surface transportation is an increasingly attractive target for terrorists seeking to inflict damage on the American public and the U.S. economy, which depends heavily on the free movement of people and goods via transportation systems. It is in light of this, that I am convening a joint Subcommittee hearing on the security of our surface transportation sector. At the hearing, the Subcommittee will hear from a number of federal and local stakeholders on how security can be improved in the surface environment. As a supplement to the testimony we will receive from TSA's witness at the hearing, I request answers to the following questions:

1. What are the primary threats facing surface transportation security?
2. What proactive actions has the Department of Homeland Security (DHS) and TSA taken to respond to the unique vulnerability of surface transportation?
3. How are information-sharing enterprises, such as the state and local fusion centers and FBI-led Joint Terrorism Task Forces utilized to protect surface transportation and what is TSA's role in this effort?

4. How has TSA worked to improve coordination between federal, state, and local entities and what is the primary mechanism by which TSA communicates threat information to its transit agency stakeholders?
5. Does TSA conduct regular risk assessments on the nation's surface transportation sector, as a whole, as well as on specific transit agencies? If so, how often, and are the results of such assessments shared with stakeholders?
6. What is the current deployment focus of TSA-led Visible Intermodal Prevention and Response (VIPR) teams? Are they focused more heavily on surface or aviation systems?
7. How does TSA measure the security contribution of its surface inspectors program? What sort of surface-specific training do these inspectors receive to qualify them to assess the unique security challenges of the surface transportation environment?
8. What technological advancements is DHS/TSA investing in to enhance the screening, vetting, and security of surface transportation travelers and workers?

I look forward to working with you to close vulnerabilities in the surface transportation sector and ensure that TSA is doing everything possible to keep the traveling public safe in every mode of transportation. I appreciate your attention to this matter, and should you have any questions, please do not hesitate to contact me or my Committee staff[.]

Sincerely,

JOHN KATKO,
Chairman, Subcommittee on Transportation Security.

Mr. KATKO. I now recognize a Member of the Subcommittee on Transportation Security, the gentlewoman from New York, Miss Rice, for an opening statement.

Miss RICE. Thank you, Mr. Chairman. Thank you for convening this hearing. I also want to thank the witnesses for joining us here today to discuss the evolving threats to our Nation's surface transportation system.

Since the beginning of the 114th Congress, this subcommittee has mainly focused its attention on aviation security. But with all modes of surface transportation carrying well over 10 billion passengers each year and more than 2.5 million miles of pipeline carrying hazardous liquids and natural gases, I am confident we can all agree that surface transportation security is equally as important. So I am pleased to have the opportunity today to address the security challenges facing the surface transportation sector as we assess the evolving threats of terrorism.

Last month, four individuals, including three brave Americans, thwarted a potential mass shooting when a man carrying a machine gun and a knife boarded a high-speed train traveling from Amsterdam to Paris. That should serve as a vivid reminder to us all that the threat of terrorism is just as real on our trains as it is on our planes, and we must be prepared to confront and neutralize that threat wherever we may find it.

We must work together to rigorously assess our surface transportation systems and ensure that we have adequate procedures in place to respond to a terrorist attack on an American pipeline or mass transit system. We must have reliable, comprehensive security plans in place for a wide range of scenarios. We must have seamless communication between Government entities and transit agencies. We must continue to encourage the public to be vigilant at all times, because, as we saw last month in France, that can be the difference between life and death.

I am very eager to hear what both the TSA and the private sector are doing to guarantee the safety of our citizens, not only those who travel on our mass transit systems, but also those who live

near pipelines and freight railroads, as well as those who travel every day on our highways.

I am also eager to hear what front-line security training has currently provided to our transit system workers, given that TSA has not yet fulfilled the statutory mandate that they develop and implement security training requirements for public transportation rail and bus workers.

In July, Ranking Member Thompson and I asked GAO to review TSA's surface inspection program. Specifically, we asked about the roles and responsibilities of those inspecting surface transportation, how the structure of the inspection program aligns with TSA's mission, and what steps are being taken to measure its effectiveness. I look forward to seeing the results of that review upon its completion, and I would welcome any additional information about those questions that our witnesses could provide today.

Mr. Chairman, thank you again for convening this hearing. I look forward to a productive dialogue today. I yield back the balance of my time.

[The statement of Miss Rice follows:]

STATEMENT OF RANKING MEMBER KATHLEEN RICE

SEPTEMBER 17, 2015

Thank you, Mr. Chairman. And thank you for convening this hearing.

I also want to thank the witnesses for joining us today to discuss the evolving threats to our Nation's surface transportation systems.

Since the beginning of the 114th Congress, this subcommittee has mainly focused its attention on aviation security.

But with all modes of surface transportation carrying well over 10 billion passengers each year, and more than 2.5 million miles of pipeline carrying hazardous liquids and natural gases, I'm confident we can all agree that surface transportation security is equally as important.

So I'm pleased to have the opportunity today to address the security challenges facing the surface transportation sector as we assess the evolving threats of terrorism.

Last month, four individuals, including three brave Americans, thwarted a potential mass shooting when a man carrying a machine gun and a knife boarded a high-speed train traveling from Amsterdam to Paris.

That should serve as a vivid reminder to us all that the threat of terrorism is just as real on our trains as it is on our planes—and we must be prepared to confront and neutralize that threat wherever we may find it.

We must work together to rigorously assess our surface transportation systems and ensure that we have adequate procedures in place to respond to a terrorist attack on an American pipeline or mass transit system.

We must have reliable, comprehensive security plans in place for a wide range of scenarios. We must have seamless communication between Government entities and transit agencies. We must continue to encourage the public to be vigilant at all times—because as we saw last month in France, that can be the difference between life and death.

I am very eager to hear what both the Transportation Security Administration and the private sector are doing to guarantee the safety of our citizens—not only those who travel on our mass transit systems, but also those who live near pipelines and freight railroads, as well as those who travel every day on our highways.

I'm also eager to hear what front-line security training is currently provided to our transit system workers, given that TSA has not yet fulfilled the statutory mandate that they develop and implement security training requirements for public transportation, rail, and bus workers.

In July, Ranking Member Thompson and I asked the Government Accountability Office to review TSA's surface inspection program.

Specifically, we asked about the roles and responsibilities of those inspecting surface transportation, how the structure of the inspection program aligns with TSA's mission, and what steps are being taken to measure its effectiveness.

I look forward to seeing the results of that review upon its completion, and I would welcome any additional information about those questions that our witnesses could provide today.

Mr. Chairman, thank you again for convening this hearing.

I look forward to productive dialogue today, and I yield back the balance of my time.

Mr. KATKO. Thank you, Miss Rice.

The Chair now recognizes the Chairman of the Subcommittee on Counterterrorism and Intelligence, Mr. King, for any statement he may have.

Mr. KING. Thank you, Mr. Chairman. I want to thank you for holding this joint hearing with the Counterterrorism and Intelligence Subcommittee today on terror threats to surface transportation.

If I may be allowed, I would like to acknowledge the fact that yesterday the House passed H.R. 720, which you sponsored, to require all airports and other surface transportation hubs to establish procedures responding to security threats such as active shooters. This was in response to the tragic murder of TSA screener Gerardo Hernandez, who was shot and killed back in November 2013 at LAX. It will now be sent to the President for signature. I want to take this opportunity to congratulate you on this passage of your first public law. It took me a lot longer to get there than it did you. So congratulations.

Mr. KATKO. Thank you very much.

Mr. KING. By the way, as part of that, I think the fact that you are holding this hearing today, this joint hearing, is emblematic of the dedication you have on this, as does Miss Rice and Ranking Member Higgins.

With the recent attempt by a terrorist on a high-speed rail in Europe to take multiple lives, we are more cognizant than ever of the vulnerability of our public transportation infrastructure. That day, as Chairman Katko mentioned, passengers were fortunate to have among them four brave Americans, including two members of America's Armed Forces, who reacted swiftly and bravely to take down the Islamist extremist who attempted to take as many lives as possible that day. But the odds are that when the next would-be terrorist attacks passengers on a train or a subway, the public may not be so fortunate to have such capable people on board who are ready to react.

The easy access to rail transportation is one of the features that makes it so popular. Compared with air travel, most of us individually appreciate the relative ease of using subways, like the Metro here in the District of Columbia or MTA in New York or commuter rail, such as Long Island Railroad or Metro-North. Everyone values and enjoys simple and easy access. However we have seen the vulnerability inherent in easy access in most transit services, including we have seen that in London, Mumbai, Madrid, Tokyo, and now in Paris. I think as a New Yorker, where we have in New York City alone literally thousands of train station entrances and exits, combine that with Grand Central Station, Penn Station, you realize just how challenging this is.

With ISIS urging supporters to carry out attacks in the United States, we have to continue to evaluate the threat, vulnerability, and related security measures within our security transportation

infrastructure. I look forward to hearing from the witnesses about efforts to deter and prevent attacks, as well as how we are balancing the efficiency of public transit with security.

A key issue is how the Federal Government is assisting State, local, and regional partners to better protect the traveling public against the threat of terrorism on America's public transportation and commuter rail systems.

Thank you, Mr. Chairman. I look forward to the testimony. I yield the balance of my time.

Mr. KATKO. Thank you, Mr. King.

The Chair now recognizes the Ranking Minority Member of the Subcommittee on Counterterrorism and Intelligence, Mr. Higgins, for any statement he may have.

Mr. HIGGINS. Thank you, Mr. Chairman, for holding this hearing to examine options for enhancing the safety and security across our surface transportation sectors.

The attacks of 9/11 focused and exploited the weaknesses inherent in our aviation security to perpetuate one of the worst attacks on United States soil. However, we must remember other modes of transportation have been and remain a top priority for terrorist groups world-wide and their affiliates. There have been devastating terrorist attacks against all modes of surface transportation across the globe, including train bombings in Belarus, India, Russia, Spain, and the United Kingdom, and most recently a shooting on a train traveling from Amsterdam to Paris.

While there was not been a successful transportation-related attack by al-Qaeda in the United States since 9/11, there have been a number of thwarted plots. My concern with this issue led me to introduce legislation in July entitled the Known Chemical, Biological, Radiological, and Nuclear Threats to Transportation Act.

The Department of Energy plans to begin transporting highly enriched uranium liquid from Canada to South Carolina next year. The Department of Energy proposes to transport this waste, which is far more radioactive than spent nuclear fuel, across the Northern Border at the Peace Bridge, crossing through several States and municipalities before reaching South Carolina. An attack on one of these trucks crossing the Peace Bridge could contaminate the Great Lakes—which contains 84 percent of North America's surface fresh water—with highly radioactive material.

Moreover, an attack on a truck moving through heavily populated areas throughout the United States would have obvious and devastating consequences.

Despite these risks, the Department of Energy is about to begin importing highly radioactive material, which has never before been shipped in this manner, using outdated, pre-9/11 information that does not reflect the threats we face today.

My bill, which was advanced through my Counterterrorism and Intelligence Subcommittee today unanimously, would direct the Department of Homeland Security's Office of Intelligence and Analysis to conduct an assessment of the risks associated with the transportation of chemical, biological, nuclear, and radiological materials. The bill also mandates that the Office of Intelligence and Analysis consult and share information with the heads of other Federal agencies, including the Transportation Security Adminis-

tration, so that the assessment is informed by the most current information about homeland security threats.

As my bill continues to move through the House and the Senate, I hope to raise awareness of the security risks and protections needed within the surface transportation sector of our country.

Again, I thank Chairman King, Chairman Katko, and my fellow Ranking Member Rice for their leadership in focusing our oversight on this hearing. With that, I yield back.

[The statement of Mr. Higgins follows:]

STATEMENT OF RANKING MEMBER BRIAN HIGGINS

SEPTEMBER 17, 2015

Chairmen, I would like to thank you for holding this hearing to examine options for enhancing the safety and security across our surface transportation sectors.

The attacks of 9/11 focused and exploited the weaknesses inherent in aviation security to perpetrate one of the worst attacks on U.S. soil. However, we must remember other modes of transportation have been and remain a top priority for transnational terrorist groups world-wide and their affiliates.

There have been devastating terrorist attacks against all modes of surface transportation across the globe including train bombings in Belarus, India, Russia, Spain and the United Kingdom, and most recently, a shooting on a train traveling from Amsterdam to Paris. While there has not been a successful transportation-related attack by al-Qaeda in the United States since 9/11, there have been a number of thwarted plots.

My concern with this issue led me to introduce legislation in July titled the "Known CBRN Threats to Transportation Act." The Department of Energy plans to begin transporting highly enriched uranium liquid from Canada to South Carolina next year. The Department of Energy proposes to transport this waste, which is far more radioactive than spent nuclear fuel, across the Northern Border at the Peace Bridge, crossing through several States and municipalities before reaching South Carolina.

An attack on one of these trucks crossing the Peace Bridge could contaminate the Great Lakes, which contain 84% of North America's surface fresh water, with highly radioactive material. Moreover, an attack on a truck moving through heavily-populated areas throughout the United States would have obvious and devastating consequences.

Despite these risks, the Department of Energy is about to begin importing highly radioactive material, which has never before been shipped in this manner, using outdated, pre-9/11 information that does not reflect the threats we face today.

My bill, which was advanced through my Counterterrorism and Intelligence Subcommittee today unanimously, would direct the Department of Homeland Security's Office of Intelligence and Analysis to conduct an assessment of the risks associated with the transportation of chemical, biological, nuclear, and radiological materials.

The bill also mandates that the Office of Intelligence and Analysis consult and share information with the heads of other Federal agencies, including the Transportation Security Administration so that the assessment is informed by the most current information about homeland security threats.

As my bill continues to move through The House and Senate, I hope to raise awareness of the security risks and protections needed within surface transportation sector of our country.

Again, I thank Chairman King, Chairman Katko, and my fellow Ranking Member Rice for their leadership and focusing our oversight on this hearing.

With that, I yield back.

Mr. KATKO. Thank you, Mr. Higgins.

Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

Thank you, Mr. Chairman, for holding this timely and important hearing.

The Transportation Security Administration was established shortly after the terrorist attacks of 2001.

While the name of the agency implies that its mission is to help secure all modes of transportation, in practice, most of TSA's attention and resources are dedicated to aviation security.

TSA has an important statutory role to play in securing freight rail, highway and motor carriers, pipelines, and mass transit and passenger rail systems.

Last month's attempted terrorist attack on a passenger train in Europe should remind us all of the need to focus on and allocate resources to securing all modes of transportation.

On August 21, 2015, a terrorist opened fire on a train full of passengers en route from Amsterdam to Paris.

Thanks, in large part, to the selfless efforts of four individuals, including three Americans, the attacker was subdued and the attack—which could have been much worse—was ended.

With this event fresh in our minds, it is necessary for us to discuss what TSA can be doing to bolster the Nation's non-aviation transportation systems.

The Implementing Recommendations of the 9/11 Commission Act of 2007, which I authored, directed TSA to take specific actions to address various issues and vulnerabilities within the surface transportation sector.

In addition to requiring security assessments for public transportation systems, it directed TSA to issue regulations for a public transportation security training program.

This plan would provide public transportation employees, including front-line employees, with the training necessary to properly respond in the event of a security threat.

The law gave TSA interim authority to issue final regulations and required TSA to have a detailed program in place by August 1, 2008.

Needless to say, to this date—nearly 8 years later—the front-line training requirement still has not been implemented by TSA.

It is necessary that the men and women who work to ensure that these transportation systems are trained to react to and mitigate the effects of a terrorist attack or security incident; they are a vital layer of security.

TSA cannot implement security initiatives within the surface transportation sector alone.

In fact, it takes a comprehensive public-private partnership to effectively address vulnerabilities.

Given today's panel, we will gain a good understanding of the way that TSA communicates and works with private-sector entities to prepare for security events and implement security measures.

I expect that Chief Hanson of Amtrak and Mr. Diaz of the Metropolitan Transportation Authority in New York will give valuable insight and perspective regarding the procedures in place to keep travelers safe, as they protect and transport millions of passengers every day, and I thank them for being here.

I also look forward to hearing from Ms. Grover about TSA's progress in addressing issues involving rail security incident reporting requirements, as well as the system TSA utilizes to integrate stakeholder feedback into their surface operations.

Lastly, I look forward to hearing about TSA initiatives in place to address all vulnerabilities and issues associated with surface modes of transportation from Mr. Mayenschein.

I thank all witnesses for being here today, and look forward to the dialogue.

With that, Mr. Chairman, I yield back the balance of my time.

Mr. KATKO. We are pleased to have with us today a group of distinguished witnesses to speak on this very important topic. Let me remind the witnesses that their entire written statements will appear in the record. I simply want to caution you that we are going to be interrupted at some point for votes today. So the more brief the opening statements, it would be probably most productive for us. So I would appreciate you accommodating us on that.

Our first witness today is Mr. Eddie Mayenschein, who serves as assistant administrator in the Office of Security Policy and Industry Engagement at the Transportation Security Administration. Previously, Mr. Mayenschein served as an executive at United Airlines and was vice president of flight operations for Ameriflight, the world's largest Part 135 airline.

The Chair now recognizes Mr. Mayenschein to testify.

STATEMENT OF EDDIE MAYENSCHEIN, ASSISTANT ADMINISTRATOR, OFFICE OF SECURITY POLICY AND INDUSTRY ENGAGEMENT, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. MAYENSCHEIN. Good afternoon, Chairman Katko, Ranking Member Rice, Chairman King, and Ranking Member Higgins, distinguished Members of the committee. I appreciate the opportunity to appear before you today to discuss the Transportation Security Administration's role in surface transportation security.

The surface transportation enterprise is massive. It is a huge challenge to secure surface transportation systems in a society where the free movement of people and commerce is not only expected, it is a valued way of life. Unlike the aviation realm where TSA conducts security operations, TSA's role in surface is focused primarily on oversight, cooperation, and regulation.

Since its inception, TSA has worked collaboratively with surface transportation operators, security partners, and the Federal interagency to ensure appropriate security posture. Our emphasis has been four-fold: Intelligence and information, sharing transportation security grants, training and exercises, and operational augmentation.

Since 2002, TSA has valued collaborative information sharing among interagency and industry partners. Intelligence and information-sharing efforts are conducted through entities such as the Transit Policing and Security Peer Advisory Group, or the PAG, consisting of chiefs of police and security directors from 27 entities, including the largest U.S. public transportation systems, also Canada and the United Kingdom. We also host forums such as the Annual Mass Transit and Passenger Rail Security Roundtable and monthly industry operator conference calls in all modes.

TSA advises FEMA for DHS surface transportation grants and develops risk-based funding priorities on security initiatives in surface transportation. Since 2006, $2.3 billion has been made available via the various security grant programs.

Through close work with our partners, we provide resources for security exercises and training. With Congress' help, TSA created the Intermodal Security Training and Exercise Program, or I–STEP, to assist surface entities testing and evaluating their security plans and their ability to respond to incidents. Most recently, an I–STEP exercise was conducted in Philadelphia to prepare for the papal visit.

As was the practice first initiated by DOT's Federal Transit Administration, TSA also works very closely with our stakeholders to update and disseminate recommended security guidelines, such as security action items for mass transit, highway and freight rail, motor coach security best practices, and pipeline security smart practice observations.

Lastly, each of the surface modes has developed or is developing handbooks, guides, and/or security DVDs, Web-based training addressing such subjects as sabotage, IED detection and response, and highlights the DHS-sponsored Run, Hide, Fight active-shooter training.

The TSA First Observer program trains highway professionals to observe, assess, and report potential security and terrorism inci-

dents. Beginning in 2004, and also with Congressional support and authorization, TSA expanded the National Explosive Detection K–9 Program to include mass transit, passenger rail systems, and ferries. Currently, 139 transit maritime K–9 teams are deployed to high-risk systems.

In the aftermath of the terrorism incidents in London's transit system in 2005, TSA created the Visible Intermodal Prevention and Response, the VIPR team concept, to augment law enforcement and security personnel to enhance security in the Nation's transportation system. Currently, 31 VIPR teams are based in 20 high-risk locations throughout the Nation.

TSA appreciates the collaborative working relationship we have with our industry partners, including those from Amtrak and New York MTA, who are testifying on this panel today.

The recent incident in France is a reminder that we collectively must remain attentive to world-wide threats and incidents. Following that incident, transit and law enforcement agencies across the Nation participated in an Amtrak-sponsored operation known as RAILSAFE, which is conducted several times each year to deter terrorist activity through unpredictable security activities.

I thank the committee Members for their interest, and most importantly, their demonstrated support of these issues, and I look forward to answering your questions.

[The prepared statement of Mr. Mayenschein follows:]

PREPARED STATEMENT OF EDDIE MAYENSCHEIN

SEPTEMBER 17, 2015

Good afternoon Chairman Katko, Ranking Member Rice, Chairman King, Ranking Member Higgins, and distinguished Members of the committee. I appreciate the opportunity to appear before you today to discuss the Transportation Security Administration's (TSA) role in surface transportation security.

TSA is a high-performing counterterrorism agency, applying a layered, intelligence-driven and risk-based approach to protect the Nation's transportation systems, including aviation, mass transit and passenger rail, freight rail, highway and motor carrier, and pipeline. Additionally, TSA leverages its core competencies in credentialing, explosives detection, and intermodal security to support the U.S. Coast Guard as lead agency for maritime security. With its surface transportation programs, TSA strengthens and enhances the security of a complex transportation network through cooperative and collaborative efforts with significant sector operators to develop best practices and share information.

SURFACE TRANSPORTATION BACKGROUND

TSA could not accomplish this essential mission without intelligence analysis and information sharing, explosives detection canine teams, Visible Intermodal Prevention and Response (VIPR) teams, and our industry partners voluntarily adopting security improvements and sharing best practices with each other and with TSA. This collaborative "whole community" approach helps to ensure that both TSA and industry resources are applied efficiently and have the highest efficacy in reducing risk to the Nation's transportation systems.

Protecting the Nation's transportation systems to ensure freedom of movement for people and commerce is crucial to every American's daily life. There are over 12,000 individual companies or agencies that operate within the five modes of the surface transportation landscape. More than 500 individual freight railroads operate on nearly 140,000 miles of track carrying essential goods. Eight million large capacity commercial trucks, and almost 4,000 commercial bus companies travel on the 4 million miles of roadway in the United States and more than 600,000 highway bridges and through 350 tunnels greater than 100 meters in length. In the mass transit and passenger rail mode there are approximately 7,300 organizations representing a wide range of systems from very small bus-only systems in rural areas to very large multi-modal systems in urban areas. Surface transportation operators carry approxi-

mately 750 million intercity bus passengers and 10 billion passenger trips on mass transit each year. The pipeline industry consists of more than 2.5 million miles of pipelines, owned and operated by approximately 3,000 private companies, which transport natural gas, refined petroleum products and other commercial products throughout the United States.

TSA oversees the development and implementation of risk-based security initiatives for these different modes of surface transportation in coordination with our security partners. As part of its security and counterterrorism mission, TSA works with private and municipal operator stakeholders to formulate policies and practices that improve security operations in their day-to-day environment. The Surface Division conducts analysis of transportation security and threat issues from both a long-term strategic perspective and near real-time analysis through data collected from TSA inspections and assessments. These analyses facilitate the assessment of risk in each surface mode and guide the development of risk reduction plans and initiatives. For instance, in 2007 our review of the industry scores in the training category of the BASE assessments indicated a potential vulnerability. TSA addressed this vulnerability by modifying the Transit Security Grants Program to prioritize front-line employee training.

These activities, such as Security Awareness Messages (SAMs), provide our security partners with a menu of risk mitigation options they can implement based on the threat and their specific capabilities. Additionally, we develop, evaluate, approve, and implement surface transportation security initiatives to ensure that security guidance, policies, and regulations issued by TSA are risk-based, outcome-oriented, and effective in reducing risk.

COLLABORATION WITH FEDERAL, STATE, LOCAL, TRIBAL, AND PRIVATE ENTITIES

TSA maintains strong working relationships with modal administrations of the Department of Transportation (DOT). The Department of Transportation is the co-Sector Specific Agency with TSA for the transportation sector and routinely communicates, coordinates, and collaborates on the harmonization of safety and security priorities. This coordination includes working directly with the Federal Railroad Administration, the Federal Transit Administration, the Federal Highway Administration, the Federal Motor Carrier Safety Administration, and the Pipeline and Hazardous Materials Safety Administration. As part of the DHS-led Critical Infrastructure Partnership Advisory Council framework, DOT and TSA co-chair Government Coordinating Councils for surface transportation modes, including freight rail, mass transit and passenger rail, highway and motor carrier, and pipelines. Coordinated activities include collaboration on new and existing regulations, conducting security assessments and analysis of data, developing and conducting training and exercises to address counterterrorism and all-hazards, and sharing Unclassified and Classified information as appropriate.

TSA engages with State, local, Tribal, and private-sector partners to identify ways to reduce vulnerabilities, assess risk, and improve security through collaborative and voluntary efforts while maintaining the flow of people and commerce. Planning initiatives and policies in coordination with our stakeholders is of utmost importance. TSA works with industry operators to ensure efforts and resources are appropriately directed towards reducing risk to the surface transportation network and infrastructure. Collaboration with those stakeholders is particularly important, and achieved in part through formal structures like the DHS-led Critical Infrastructure Partnership Advisory Council framework, Sector Coordinating Councils, and other industry-centric organizations such as the Mass Transit Policing and Security Peer Advisory Group.

Through these established networks and other informal channels, TSA collaborates with security and corporate leadership of the industry and municipal operator stakeholders in the pursuit of policy that reduces risk, including implementation of exercises, physical and cyber hardening measures, and operational deterrence activities. We also work very closely with our stakeholders in the development and dissemination of recommended practices, such as Security Action Items (SAIs) for mass transit, highway, and freight rail; motor-coach security best practices, and the Pipeline Security Smart Practice Observations. Through these networks, we have also established robust information sharing procedures and capabilities, such as the distribution of SAMs, the establishment of monthly stakeholder conference calls, and the dissemination of intelligence and threat information through modal Information Sharing and Analysis Centers (ISACs).

On the passenger rail side, TSA and Amtrak partner on programs such as Regional Alliance Including Local, State, and Federal Efforts (RAILSAFE) to deter terrorist activity through unpredictable security activities. This program also incor-

porates other rail, transit, and local law enforcement agencies and involves counter-terrorism activities such as increased station and right-of-way patrols, greater security presence on trains and at stations, explosive detection sweeps using canine teams, and random passenger bag inspections. Participating entities conduct these activities at local and regional high-risk transit locations to disrupt potential terrorist activities and reconnaissance as part of the layered approach to security. On average, more than 40 States and over 200 agencies, including TSA's VIPR teams, participate RAILSAFE activities.

Through highway and motor carrier security programs, TSA has provided multiple voluntary initiatives to industry through forums and other communications, including security action items and training, which focus on over-the-road buses that service high-threat urban areas, trucks carrying hazardous materials, and student transportation. Additionally, TSA coordinates and collaborates with the Department of Transportation to develop and implement a National Strategy for Bridge and Tunnel Security based on the United States Army Corps of Engineers' (USACE) vulnerability assessments. As a result, and working with USACE, TSA has assessed 100 percent of all high-risk bridges and tunnels, and has provided 81 percent of the remediation recommendations to asset owners. The final 19 percent of reports are in the process of being completed and will be shared within the next 12 months.

For the transport of hazardous cargo on the Nation's roadways, TSA conducts security threat assessments on professional drivers with Commercial Drivers Licenses who seek endorsement to haul hazardous materials. Only those applicants who have been successfully vetted and have received a TSA-approved Security Threat Assessment (STA) are allowed to transport such hazardous materials.

We work very closely with the pipeline industry on identifying and improving cybersecurity vulnerabilities, including coordinating a number of Classified briefings to increase awareness of the threat. TSA's involvement in the Pipeline Corporate Security Review (CSR) and Critical Facility Security Review (CFSR) program continues to help our pipeline stakeholders improve their organization-wide and critical infrastructure-specific security postures.

As an example of our close working relationships with the industry, TSA recently successfully launched the Loaned Executive Program aimed at providing senior-level transportation security officials with first-hand experience of the Transportation Security Administration's various counter-terrorism and risk reduction roles in enhancing industry security is providing real-world experience and detailed industry exposure to TSA's surface security programs and policies. The program, which began as a pilot last September, has seen executives from Amtrak, Washington Metropolitan Area Transit Authority, and Bay Area Rapid Transit Authority participate in the program so far.

TSA provides the Federal Emergency Management Agency (FEMA) with subject-matter expertise to assist in the development of transportation security Notice of Funding Opportunities (grants) for surface transportation owners and operators. These FEMA grants support transportation risk mitigation by applying Federal funding to critical security projects with the greatest security effects. Between fiscal years 2006 and 2014, over $2.2 billion in transportation security grant funding was awarded to freight railroad carriers and operators, over-the-road bus operators, the trucking community, and public mass transit owners and operators, including Amtrak, and their dedicated law enforcement providers. TSA continuously reviews the grant program framework and makes recommendations to FEMA, ensuring funding priorities are based on identified or potential threat and vulnerabilities identified through TSA assessment programs such as the Baseline Assessment for Security Enhancement (BASE) program, together with consideration of potential consequences. As a result, DHS is able to direct grant funds to activities that have the highest efficacy in reducing the greatest risk, such as critical infrastructure vulnerability remediation, equipment purchases, anti-terrorism teams, mobile screening teams, explosives detection canine teams, training, drills/exercises, and public awareness campaigns.

TRAINING AND EXERCISES

TSA works closely with our transportation stakeholders to provide resources for security training and exercises. Through a National review of assessments, TSA identified areas where we could assist transportation entities in providing better security training to their front-line employees. As such, TSA prioritized the development and distribution of security training resources for surface transportation front-line employees through channels such as TSA-produced training modules and making recommendations to adjust grant program priorities. TSA's First Observer™ program trains highway professionals and other security entities, such as those re-

sponsible for providing parking and facility security at major sporting arenas and venues, to observe, assess, and report potential security and terrorism incidents. Since fiscal year 2006, over $141 million in grant funding has been awarded to mass transit, freight rail, and over-the-road bus operators for security training, including over $129 million through the Transit Security Grant Program for mass transit agencies and Amtrak; over $6.9 million through the Freight Rail Security Grant Program for freight rail carriers; and $5.4 million through the Intercity Bus Security Grant Program for over-the-road bus operators. Additionally, we have developed and distributed an array of mode-specific training products for front-line employees. With this targeted effort on security training, TSA has seen assessment results related to security training improve across all modes of surface transportation. As an example, since 2007, the percentage of grant-eligible mass transit agencies that have a sound security training program based on their BASE scores has increased from 19% to 66%. Also, as a sub-set, the percentage of agencies in the higher-risk regions with sound security training programs has increased from 27% to 78%.

With regard to exercises, TSA collaborates with industry through our Intermodal Security Training and Exercise Program (I–STEP) across all modes of surface transportation. TSA facilitates I–STEP exercises to help surface transportation entities test and evaluate their security plans, including prevention and preparedness capabilities, and their ability to respond to threats and cooperate with first responders from other entities. Entities that receive an I–STEP exercise are selected through an extensive review process based on risk, which looks at elements such as assessment results, emerging threats as identified through intelligence resources. As new threats emerge, I–STEP scenarios are updated to ensure our industry partners are prepared to exercise the most appropriate countermeasures.

ASSESSMENTS AND INSPECTIONS

TSA also plays a role in surface transportation security through voluntary assessments and regulatory compliance inspections. The Surface Division works closely with TSA's Office of Security Operations (OSO), which conducts both voluntary assessments and required regulatory compliance inspections.

TSA conducts approximately 10,000 regulatory inspections of freight railroads each year to ensure compliance with regulations requiring the secure exchange of custody of rail cars carrying Rail Security Sensitive Materials, as well as reporting significant security concerns and providing location and shipping information of certain rail shipments to TSA.

OSO's Surface Transportation Security Inspectors conduct a thorough security program assessment of mass transit agencies to include Amtrak, and over-the-road bus operators through the BASE program. BASE assessments are conducted with emphasis on the 100 largest mass transit and passenger railroad systems measured by passenger volume, which account for over 95 percent of all users of public transportation. Results of these assessments feed into resource allocation decisions, including I–STEP exercises and grant funding, to ensure that the higher-risk entities with the greatest need receive priority consideration for available resources. For instance, in 2007 our review of the industry scores in the training category of the BASE assessments indicated a potential vulnerability. TSA addressed this vulnerability by modifying the Transit Security Grants Program to prioritize front-line employee training.

Assessments and inspections in surface transportation are not limited to rail and highway operations. In pipeline mode, for example, the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. No. 110–53) required TSA to develop and implement a plan for inspecting the critical facilities of the top 100 pipeline systems in the Nation. These required inspections were conducted between 2008 and 2011 through the Critical Facility Inspection program, with regular recurring reviews now being conducted through TSA's Critical Facility Security Review program.

CONCLUSION

TSA works collaboratively with surface transportation industry partners to develop and implement programs while enhancing security and mitigating the risk to our Nation's surface transportation systems while promoting commerce. I want to thank the committee for its continued assistance to TSA and for the opportunity to discuss our work in partnering with the surface transportation industry to provide better security to the American people. Thank you, and I look forward to your questions.

Mr. KATKO. Thank you, Mr. Mayenschein, for your testimony. We appreciate you being here today.

Our second witness is well-known to us, Ms. Jennifer Grover, who currently serves as the director for transportation security and Coast Guard issues on U.S. Government Accountability Office's Homeland Security and Justice Team.

Ms. Grover, I just want to note that you have provided great information for us in both a secure and a nonsecure setting in the past, and I look forward to hearing from it again today. I encourage you, as always, to be as frank and forthright as possible with issues so that we can best address them moving forward.

So what that, I recognize you to testify.

STATEMENT OF JENNIFER GROVER, DIRECTOR, TRANSPORTATION SECURITY AND COAST GUARD ISSUES, HOMELAND SECURITY AND JUSTICE TEAM, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. GROVER. Thank you. Good afternoon. I am pleased to be here today to discuss TSA's efforts to secure the U.S. surface transportation system.

As many of you have already noted, rail and transit systems, pipelines, and the Nation's highway transportation system are inherently vulnerable to attack and difficult to secure because they are open systems with multiple access points, where people and vehicles can generally move about freely. In this situation, good intelligence and robust communication about possible threats becomes critically important.

Compared to aviation, where TSA has a direct role in providing security, TSA's role in surface transportation security is indirect. For example, TSA contributes to surface transportation security by providing industry with recommended security standards and conducting voluntary security assessments.

TSA is also responsible for gathering information and sharing intelligence about potential threats. Specifically, TSA requires U.S. rail agencies to report all rail security incidents, with the intent of allowing TSA to analyze the data, identify new threats, and alert the rail industry and law enforcement.

For this to work, though, TSA has to receive consistent and accurate information on these rail incidents. They have to have a data management system in place to capture the information, to conduct appropriate analysis, and have effective data-sharing mechanisms. TSA has recently taken steps to improve in all of these areas.

In 2012, GAO found that TSA headquarters had not provided guidance to local TSA officials, called surface inspectors, about the types of rail security incidents that rail systems had to report, which led to inconsistent reporting. As a result, the number of incidents per million riders reported by 7 passenger rail systems ranged from less than 1 to 23 during 2011.

Now, some variation is always to be expected. But in this case passenger rail officials told us that they had received inconsistent feedback from TSA surface inspectors about what should be reported, particularly for incidents involving weapons. We also found that TSA's enforcement of the reporting requirement varied, with some rail systems not inspected at all over an 18-month period and

TSA inspectors taking action against some rail systems but not others when both rail systems failed to report the same type of incident.

In addition, the quality of TSA's data was poor, as its data management system didn't capture all incidents and was prone to data entry errors. Due to other technical limitations, TSA couldn't provide basic information, such as the number of incidents by type or rail system. Without this type of analytic ability, TSA faced challenges in identifying patterns or trends in the data as the system was intended to do.

Finally, in June 2014, GAO also found that surface transportation stakeholders varied in their level of satisfaction with TSA's security-related information sharing, but TSA did not have a systematic process for collecting and addressing stakeholder feedback to ensure that the information they were providing was of value.

In response to our recommendations on these issues, TSA provided guidance to surface inspectors and rail systems to clarify reporting requirements and took steps to enhance the consistency of its inspection process. TSA has also made improvements to capture data on previously-unreported security incidents and changed the data system to improve its analytic capabilities. In addition, TSA has developed a new process to document and respond to stakeholder feedback on its efforts.

Collectively, these changes addressed the intent of our recommendations. If TSA implements them effectively going forward, they will help to ensure that the rail security incident reporting process is consistently implemented and that TSA has the tools and information necessary to develop a useful, comprehensive, and accurate picture of security incidents, as well as developing trends or patterns.

Thank you for the opportunity to testify. I look forward to your questions.

[The prepared statement of Ms. Grover follows:]

PREPARED STATEMENT OF JENNIFER GROVER

SEPTEMBER 17, 2015

GAO HIGHLIGHTS

Highlights of GAO–15–205T, a testimony before the Subcommittees on Transportation Security and Counterterrorism and Intelligence, Committee on Homeland Security, House of Representatives.

Why GAO Did This Study

The U.S. surface transportation system's size and importance to the country's safety, security, and economic well-being make it an attractive target for terrorists. Within the Federal Government, TSA—a component of the Department of Homeland Security—is the primary Federal agency responsible for overseeing and enhancing the security of the surface transportation system. A key component of this responsibility is ensuring that security-related information is collected, analyzed, and shared effectively across all modes, including rail. In 2008, TSA issued a regulation requiring U.S. passenger rail agencies to report all potential threats and significant security concerns to TSA, among other things.

This testimony addresses the extent to which TSA has: (1) Developed systematic processes for integrating stakeholder feedback about security-related information it provides and analyzing trends in reported rail security incidents, and (2) ensured consistent implementation of rail security incident reporting requirements. This statement is based on related GAO reports issued in June 2014 and December 2012, including selected updates on TSA's efforts to implement GAO's prior recommenda-

tions related to rail security and information sharing. For the selected updates, GAO reviewed related documentation, including tools TSA developed to provide oversight. GAO also interviewed TSA officials.

What GAO Recommends

GAO is making no new recommendations in this statement.

SURFACE TRANSPORTATION SECURITY.—TSA HAS TAKEN STEPS DESIGNED TO DEVELOP PROCESSES FOR SHARING AND ANALYZING INFORMATION AND TO IMPROVE RAIL SECURITY INCIDENT REPORTING

What GAO Found

In June 2014, GAO found that the Transportation Security Administration (TSA) did not have a systematic process for incorporating stakeholder feedback to improve security-related information sharing and recommended that TSA systematically document and incorporate stakeholder feedback. TSA concurred with this recommendation and, in April 2015, TSA developed a standard operating procedure to help ensure proper evaluation and consideration of all feedback TSA receives. In December 2012, GAO found TSA had made limited use of the rail security incident information it had collected from rail agencies, in part because it did not have a systematic process for conducting trend analysis. TSA's purpose for collecting this information was to allow TSA to "connect the dots" through trend analysis. However, the incident information provided to rail agencies by TSA was generally limited to descriptions of specific incidents. As a result, officials from passenger rail agencies GAO spoke with reported that they generally found little value in TSA's incident reporting requirement. On the basis of these findings, GAO recommended that TSA establish a systematic process for regularly conducting trend analysis of the rail security incident data. Although GAO has not assessed the effectiveness of TSA's efforts, by August 2013, TSA had developed a new analysis capability that, among other things, produces Trend Analysis Reports from the incident data.

In December 2012, GAO found that TSA had not provided consistent oversight of its rail security reporting requirement, which led to variation in the types and number of passenger rail security incidents reported. Specifically, GAO found that TSA headquarters had not provided guidance to local TSA inspection officials, the primary TSA points of contact for rail agencies, about the types of rail security incidents that must be reported, which contributed to inconsistent interpretation of the regulation. The variation in reporting was compounded by inconsistencies in compliance inspections and enforcement actions, in part because of limited utilization of oversight mechanisms at the headquarters level. GAO also found that TSA's incident management data system, WebEOC, had incomplete information, was prone to data entry errors, and had other limitations that inhibited TSA's ability to search and extract basic information. On the basis of these findings, GAO recommended that TSA: (1) Develop and disseminate written guidance on the types of incidents that should be reported, (2) enhance existing oversight mechanisms for compliance inspections and enforcement actions, (3) establish a process for updating WebEOC with previously-unreported incidents, and (4) develop guidance to reduce data entry errors. TSA concurred with these recommendations and has taken actions to implement them. Specifically, in September 2013, TSA disseminated written guidance to local TSA inspection officials and passenger and freight rail agencies that provides clarification about the rail security incident reporting requirement. In August 2013, TSA enhanced existing oversight mechanisms by creating an inspection review mechanism, among other things. TSA also established a process for updating WebEOC in March 2013, and in October 2014, officials reported that they have updated the guidance used by officials responsible for entering incident data to reduce data entry errors associated with incident types. Although GAO has not assessed the effectiveness of these efforts, they address the intent of the recommendations.

Chairmen Katko and King, Ranking Members Rice and Higgins, and Members of the subcommittees: I appreciate the opportunity to participate in today's hearing to discuss our work related to the Transportation Security Administration's (TSA) efforts to secure the U.S. surface transportation system, particularly those associated with passenger and freight rail.[1] The transportation system's size and importance to the country's safety, security, and economic well-being make it an attractive target for terrorists. As shown by the active-shooter incident that occurred on a train traveling from Amsterdam to Paris on August 21, 2015, rail systems are inherently

[1] The surface transportation modes include passenger rail (such as subway-type mass transit systems and intercity rail such as Amtrak), freight rail, highway and commercial vehicle, and pipeline.

vulnerable to attack in part because they rely on an open architecture that is difficult to monitor and secure because of its multiple access points; hubs serving multiple carriers; and, in some cases, lack of barriers to access. One of the critical challenges facing rail system operators—and the Federal agencies that regulate and oversee them—is finding ways to protect rail systems from potential terrorist attacks without compromising the accessibility and efficiency of rail travel.

Within the Federal Government, TSA—a component of the Department of Homeland Security (DHS)—is the primary Federal agency responsible for security in all modes of transportation, including aviation, passenger and freight rail, highway and motor carrier, maritime, and pipeline.[2] A key component of this responsibility is ensuring that information related to transportation security and potential threats across all modes is collected, analyzed, and shared effectively. Disrupted terrorist attacks in recent years, such as the April 2013 disruption of a planned attack on a passenger train operating between Toronto and New York City, highlight the importance of reporting and sharing security-related information. TSA's other responsibilities, however, vary by transportation mode. Specifically, TSA has a direct role in ensuring the security of the aviation mode through its management of a passenger and baggage screener workforce that inspects individuals and their property to deter and prevent an act of violence or air piracy. In contrast, TSA's responsibilities for securing surface transportation systems such as passenger and freight rail systems have primarily included developing National strategies, establishing security standards, and conducting assessments and inspections of surface transportation modes, while public and private-sector transportation operators are responsible for implementing security measures for their systems. TSA's annual budget further highlights the difference between TSA's roles in securing the aviation and surface transportation modes. For example, the DHS Appropriations Act, 2015, enacted March 4, 2015, appropriated $123,749,000 for surface transportation security compared with $5,639,095,000 for aviation security.[3]

My statement today addresses the extent to which TSA has: (1) Developed systematic processes for integrating stakeholder feedback about security-related information provided by the agency and analyzing trends in reported rail security incidents, and (2) ensured consistent implementation of rail security incident reporting requirements. This statement is based on related GAO reports issued in December 2012 and June 2014, including selected updates on TSA's efforts to implement our prior recommendations related to information sharing and rail security.[4] To conduct our earlier work, among other things, we conducted a survey of 481 transportation stakeholders, including freight and passenger rail stakeholders, from November 2013 through January 2014, regarding their satisfaction with TSA's sharing of security-related information. We received responses from 337 stakeholders (a 70 percent response rate). We also reviewed TSA policy documents and guidance on rail security reporting requirements, and passenger rail security incident data from January 2011 through June 2012. The reports cited in this statement provide detailed information about our scope and methodology. For the selected updates, we reviewed related documentation and interviewed TSA officials on TSA's progress in addressing our recommendations. This documentation includes tools TSA developed to provide oversight of the rail security incident reporting process, guidance for TSA inspectors and rail agencies, and updates to TSA's data management system, among other things. The work upon which this statement is based was conducted in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

[2] Pub. L. No. 107–71, § 101(a), 115 Stat. 597 (2001) (codified as amended at 49 U.S.C. § 114(d)).

[3] Pub. L. No. 114–4, 129 Stat. 39, 44–46 (2015). The approximately $124 million and $5.6 billion appropriated to TSA's Surface Transportation Security and Aviation Security accounts, respectively, do not reflect amounts appropriated to TSA's Intelligence and Vetting and Transportation Security Support accounts, which also support TSA's surface and aviation security missions, as well as the $250 million in fee collections available to TSA through the Aviation Security Capital Fund to support security-related airport improvement projects and the procurement and installation of explosives detection systems for use at airports.

[4] GAO, *Transportation Security Information Sharing: Stakeholder Satisfaction Varies; TSA Could Take Additional Actions to Strengthen Efforts.* GAO–14–506 (Washington, DC: June 24, 2014), and *Passenger Rail Security: Consistent Incident Reporting and Analysis Needed to Achieve Program Objectives.* GAO–13–20 (Washington, DC: Dec. 19, 2012).

BACKGROUND

The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) directed DHS to create a plan for sharing transportation security-related information among public and private entities that have a stake in protecting the Nation's transportation system, including passenger and freight rail. This plan—first issued in July 2008—is now called the Transportation Security Information Sharing Environment (TSISE).[5] The TSISE describes, among other things, the information-sharing process. TSA disseminates security information through several information products, including reports, assessments, and briefings, among others. These products are distributed through mechanisms including the Homeland Security Information Network and mechanisms sponsored by industry, such as the Association of American Railroads' Railway Alert Network, among others.

TSA is also specifically responsible for receiving, assessing, and distributing intelligence information related to potential threats and significant security concerns (rail security incidents) related to the Nation's rail system. Specifically, in 2008, TSA issued a regulation requiring U.S. rail systems to report all rail security incidents to TSA's Transportation Security Operations Center (TSOC), among other things.[6] The TSOC is an operations center open 24 hours a day, 7 days a week, that serves as TSA's main point of contact for monitoring security-related incidents or crises in all modes of transportation. The regulation also authorizes TSA officials to view, inspect, and copy rail agencies' records as necessary to enforce the rail security incident reporting requirements.[7] This regulation is supported by TSA policies and guidance, including the Transportation Security Inspector Inspections Handbook, the National Investigations and Enforcement Manual, and the Compliance Work Plan for Transportation Security Inspectors. TSA's regulation is intended to provide the agency with essential information on rail security incidents so that TSA can conduct comprehensive intelligence analysis, threat assessment, and allocation of security resources, among other things.[8] According to the regulation, potential threats and significant security concerns that must be reported to the TSOC include bomb threats, suspicious items, or indications of tampering with rail cars, among others.[9]

Within TSA, different offices are responsible for sharing transportation security-related information and for implementing and enforcing the rail security incident reporting requirement. For instance, TSA's Office of Security Policy and Industry Engagement (OSPIE) is the primary point of contact for sharing information with private-sector stakeholders, and is responsible for using incident reports and analyses, among other things, to develop strategies, policies, and programs for rail security, including operational security activities, training exercises, public awareness, and technology. TSA's Office of Intelligence and Analysis (OIA) receives intelligence information regarding threats to transportation and designs intelligence products intended for officials in TSA, other parts of the Federal Government, State and local officials, and industry officials, including rail agency security coordinators and law enforcement officials.

The TSOC, managed by TSA's Office of Law Enforcement/Federal Air Marshal Service, is the TSA entity primarily responsible for collecting and disseminating information about rail security incidents. Once notified of a rail security incident, TSOC officials are responsible for inputting the incident information into their inci-

---

[5] Pub. L. No. 110–53, § 1203(a), 121 Stat. 266, 383–85 (2007) (codified at 49 U.S.C. § 114(u)). The TSISE was formerly called the Transportation Security Information Sharing Plan (TSISP). In fiscal year 2013, TSA renamed the plan the TSISE to reflect that the TSISE is not a part of a plan, but rather a series of processes.

[6] 49 C.F.R. §§ 1580.105, .203. These requirements generally apply to passenger and freight rail carriers, as well as rail hazardous materials shippers and rail hazardous materials receivers located within high-threat urban areas. The regulation also requires rail agencies to designate rail security coordinators, and codifies TSA's authority to conduct security inspections of rail agency property. 49 C.F.R. §§ 1580.101, .201.5 This is the only rule that TSA has issued to date regarding passenger rail security. Additional rules have been issued regarding freight rail security, specifically requirements related to rail shipments of specified hazardous materials. The Implementing Recommendations of the 9/11 Commission Act of 2007 also mandates TSA to develop and issue regulations for a public transportation security training program, among other things. Pub. L. No. 110–53, § 1408, 121 Stat. 266, 409–11 (codified at 49 U.S.C. § 1137). As of September 2015, a draft regulation had not been submitted for public comment. According to TSA, the training rule is among the agency's highest priorities, but officials did not provide a target date for when the revised regulation will be provided for public comment.

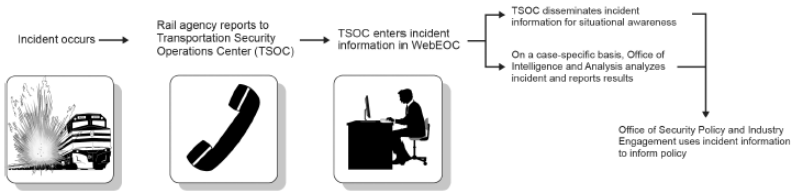
[7] 49 C.F.R. § 1580.5.

[8] 71 Fed. Reg. 76,852, 76,876 (Dec. 21, 2006).

[9] 49 C.F.R. § 1580.105(c), .203(c).

dent management database known as WebEOC, and for disseminating incident reports that they deem high priority or significant to selected TSA officials; other Federal, State, and local government officials; and selected rail agencies' law enforcement officials. Figure 1 shows the intended steps and responsibilities of TSA components involved in the rail security incident reporting process.

Figure 1: The Intended Rail Security Reporting Process



Source: GAO analysis of TSA information; Art Explosion (graphics). | GAO-15-205T

TSA's Office of Security Operations (OSO) is responsible for overseeing and enforcing the incident reporting requirement. Responsible for managing TSA's inspection program for the aviation and surface modes of transportation, the Office of Security Operations' Surface Compliance Branch deploys approximately 270 transportation security inspectors—surface (TSI–S) Nation-wide.[10] The TSI–Ss are responsible for, among other things, providing clarification to rail agencies regarding the incident reporting process and for overseeing rail agencies' compliance with the reporting requirement by conducting inspections to ensure that incidents were properly reported to the TSOC. Six regional security inspectors—surface (RSI–S) within the Compliance Programs Division are responsible for providing National oversight of local surface inspection, assessment, and operational activities.

TSA HAS DEVELOPED PROCESSES DESIGNED TO INTEGRATE STAKEHOLDER FEEDBACK AND ADDRESS GAPS IN TREND ANALYSIS

TSA Has Developed a Process Designed to Incorporate Feedback on Security-Related Information

In June 2014, we found that TSA had some mechanisms in place to collect stakeholder feedback on the products it disseminates containing security-related information and had initiated efforts to improve how it obtains customer feedback, but had not developed a systematic process for collecting and integrating such feedback.[11] Specifically, in February 2014, TSA reconvened its Information Sharing Integrated Project Team (IPT), whose charter included, among other things, milestones and time frames for developing a centralized management framework to capture stakeholder satisfaction survey data on all of TSA's security-related products and the systems used to distribute these products.[12] However, at the time of our June 2014 report, the IPT Charter did not specify how TSA planned to systematically collect, document, and incorporate informal feedback—a key mechanism used by the majority of the stakeholders we surveyed, and a mechanism TSA officials told us they utilize to improve information sharing. For instance, the rail industry provided TSA with a list of areas for emphasis in intelligence analysis in December 2012, and TSA subsequently initiated a product line focusing on indications and warnings associated with disrupted or successful terrorist attacks. TSA officials stated that they further refined one of the products as a result of a stakeholder requesting information on tactics used in foreign rail attacks. In 2013, one TSA component built a system to track informal information sharing with stakeholders at meetings and conferences,

[10] There are currently 49 TSA field offices under the Surface Compliance Branch. TSI–Ss report to assistant Federal security directors—inspection (AFSD–I), who are responsible for all inspection, compliance, and enforcement activity in their areas of responsibility. Each office is led by a Federal security director charged with the implementation of all field operational activities across all modes of transportation. For other transportation modes, as of September 2015, TSA has deployed 496 air cargo inspectors and 672 aviation regulation inspectors.

[11] GAO–14–506. Mechanisms include surveys attached to security-related information products and informal feedback collected at meetings with stakeholders.

[12] According to TSA officials, TSA formed the IPT in 2009 but planning stopped because of multiple TSA organization realignments. IPT members include OIA, OSPIE, and other TSA components, as well as external entities, such as the DHS Office of Intelligence and Analysis, stakeholders, and trade associations. One of the primary missions of the IPT is to evaluate TSA's information-sharing services across all modes of transportation.

and through e-mail, but TSA officials stated that the data were not used for operational purposes, and TSA had no plans to incorporate this system into its centralized management framework because the IPT had decided to focus its initial efforts on developing a survey mechanism.

According to our June 2014 survey results, surface transportation stakeholders were generally satisfied with TSA's security-related products and the mechanisms used to disseminate them.[13] In particular, 63 percent of rail stakeholders (70 of 111) reported that they were satisfied with the products they received in 2013, and 54 percent (59 of 110) reported that they were satisfied with security-related information-sharing mechanisms.[14] However, because TSA lacked specific plans and documentation related to improving its efforts to incorporate all of its stakeholder feedback, it was unclear how, or if, TSA planned to use stakeholder feedback to improve information sharing. As a result of these findings, we recommended that TSA include in its planned customer feedback framework a systematic process to document informal feedback, and how it incorporates all of the feedback TSA receives, both formal and informal. TSA concurred, and in response, by April 2015, had taken actions to develop these processes. Specifically, TSA developed a standard operating procedure to organize how its offices solicit, receive, respond to, and document both formal and informal customer feedback on its information-sharing efforts, which delineates a systematic process for doing so. TSA also developed a TSA-wide standard survey for its offices to use to obtain formal and informal feedback on specific products, and created an information-sharing e-mail inbox to which all survey responses will be sent, evaluated, and distributed to the appropriate office for action. We have not evaluated these actions, but if implemented effectively, we believe that TSA will now be better-positioned to meet stakeholder needs for security-related information.

TSA Efforts Should Help Address Gaps in Conducting Trend Analysis of Rail Security Incident Information

In December 2012, we found TSA had made limited use of the rail security incident information it had collected from rail agencies, in part because it did not have a systematic process for conducting trend analysis.[15] TSA's stated purpose for collecting rail security incident information was to allow TSA to "connect the dots" by conducting trend analysis that could help TSA and rail agencies develop targeted security measures. However, the incident information provided to rail agencies by TSA was generally limited to descriptions of specific incidents with minimal accompanying analysis. As a result, officials from passenger rail agencies we spoke with generally found little value in TSA's incident reporting process, because it was unclear to them how, if at all, the information was being used by TSA to identify trends or threats that could help TSA and rail agencies develop appropriate security measures. However, as we reported in December 2012, opportunities for more sophisticated trend analysis existed. For example, the freight industry, through the Railway Alert Network—which is managed by the Association of American Railroads, a rail industry group—identified a trend where individuals were reportedly impersonating Federal officials. In coordination with TSA, the Railway Alert Network subsequently issued guidance to its member organizations designed to increase awareness of this trend among freight rail employees and provide descriptive information on steps to take in response. The Railway Alert Network identified this trend through analysis of incident reporting from multiple freight railroads. In each

[13] Sixty-seven percent of surface transportation stakeholders (125 of 186) reported that they were satisfied with the security-related products they received from TSA in 2013, and 58 percent of surface transportation stakeholders (106 of 183) reported that they were satisfied with the mechanisms used to disseminate this information. Respondents who were not satisfied with TSA's security-related products or information-sharing mechanisms cited concerns that the information provided was often dated, among other issues. Survey respondents were asked to rate their organization's satisfaction using the following terms: "Very satisfied," "somewhat satisfied," "neither satisfied nor dissatisfied," "somewhat dissatisfied," "very dissatisfied," and "don't know." We use the term "satisfied" to describe organizations that indicated they were either "very satisfied" or "somewhat satisfied." Similarly, we use the term "dissatisfied" to describe organizations that indicated they were either "very dissatisfied" or "somewhat dissatisfied" with the information they received. Because satisfaction and dissatisfaction were not the only possible responses, when we report that 59 percent of respondents reported being satisfied, for example, that does not necessarily mean that 41 percent were dissatisfied.

[14] These results for rail stakeholders differ from those reported in GAO–14–506 because they represent the survey responses we received from all passenger and freight rail agencies. The "public transit" category in GAO–14–506 included 13 agencies in modes other than rail. To arrive at the numbers in this statement, we combined the responses of the 23 rail agencies in the public transit category with the responses received from 88 and 87 rail agencies in response to our questions on satisfaction with TSA products and mechanisms, respectively.

[15] GAO–13–20.

case, the incident had been reported by a railroad employee and was contained in TSA's incident management system, WebEOC.

On the basis of these findings, in December 2012, we recommended that TSA establish a systematic process for regularly conducting trend analysis of the rail security incident data, in an effort to identify potential security trends that could help the agency anticipate or prevent an attack against passenger rail and develop recommended security measures. TSA concurred with this recommendation and by August 2013 had developed a new capability for identifying trends in the rail security incident data, known as the Surface Compliance Trend Analysis Network (SCAN). SCAN is designed to identify linkages between incidents captured in various sources of data, assemble detailed information about these incidents, and accurately analyze the data to enhance the agency's ability to detect impending threats. According to TSA officials, SCAN consists of three elements: Two OSO surface detailees located at TSOC, enhanced IT capabilities, and a new rail security incident analysis product for stakeholders. According to TSA, one of the key functions of the surface detailees is to continuously look for trends and patterns in the rail security incident data that are reported to TSOC, and to coordinate with OSPIE and OIA to conduct further investigations into potential trends. As I will discuss later in this statement, TSA has also made improvements to WebEOC, including steps to improve the completeness and accuracy of the data and the ability to produce basic summary reports, which we believe should facilitate this type of continuous trend analysis.

TSA generates a Trend Analysis Report for any potential security trends the surface detailees identify from the rail security incident data. The Trend Analysis Report integrates incident information from WebEOC with information from multiple other sources, including TSA's compliance database and media reports, and provides rail agencies and other stakeholders with analysis of possible security issues that could affect operations as a result of these trends. According to TSA officials, since SCAN was established, approximately 13 Trend Analysis Reports have been produced and disseminated to local TSA inspection officials and rail agencies. Although we have not assessed the effectiveness of these efforts to better utilize rail security information, we believe these actions address the intent of our recommendation. Further, if implemented effectively, they should better position TSA to provide valuable analysis on rail security incidents and to develop recommended security measures for rail agencies, as appropriate.

TSA HAS TAKEN STEPS TO IMPROVE CONSISTENT IMPLEMENTATION OF THE RAIL SECURITY INCIDENT REPORTING PROCESS

TSA Has Taken Steps to Improve the Consistency of the Rail Security Incident Reporting Process

In December 2012, we found that TSA had not provided consistent oversight of the implementation of the rail security reporting requirement, which led to considerable variation in the types and number of passenger rail security incidents reported.[16] Specifically, we found that TSA headquarters had not provided guidance to local TSA inspection officials, the primary TSA points of contact for rail agencies, about the types of rail security incidents that must be reported, a fact that contributed to inconsistent interpretation of the regulation by local TSA inspection officials.[17] While some variation was expected in the number of rail security incidents that rail agencies reported because of differences in agency size, geographic location, and ridership, passenger rail agencies we spoke with at the time reported receiving inconsistent feedback from their local TSA officials regarding certain types of incidents, such as those involving weapons. As a result, we found that, for 7 of the 19 passenger rail agencies included in our review, the number of incidents reported per million riders ranged from 0.25 to 23.15.[18]

---

[16] GAO–13–20.

[17] For example, officials from one rail agency we spoke with had been told by their local TSA inspection officials that they were required to report all instances in which a person was hit by a train, because an individual cannot be struck by a train in the right of way without trespassing or breaching security. In contrast, officials from another rail agency told us that their agency does not report all of these incidents because they are most often intentional suicides that are unrelated to terrorism. "Local TSA inspection officials" refers to TSI–Ss and AFSD–Is.

[18] This includes incidents reported to the TSOC from January 1, 2011, through December 31, 2011, and recorded in WebEOC. However, there are limitations and errors associated with these data, which are discussed in greater detail later in this statement. Because of limitations associated with identifying the total number of incidents by agency, we limited this analysis to 7 of

Continued

This variation we identified was compounded by inconsistencies in compliance inspections and enforcement actions, in part because of limited utilization of oversight mechanisms at the headquarters level. For example, in December 2012, we found that TSA established the RSI–S position as a primary oversight mechanism at the headquarters level for monitoring rail security compliance inspections and enforcement actions to help ensure consistency across field offices. However, at the time of our report, the RSI–S was not part of the formal inspection process and had no authority to ensure that inspections were conducted consistently. We also found that the RSI–S had limited visibility over when and where inspections were completed or enforcement actions were taken because TSA lacked a process to systematically provide the RSI–S with this information during the course of normal operations. As a result, our analysis of inspection data from January 1, 2011, through June 30, 2012, showed that average monthly inspections for the 19 rail agencies in our review ranged from about eight inspections to no inspections, and there was variation in the regularity with which inspections occurred.[19] We also found that TSA inconsistently applied enforcement actions against passenger rail agencies for not complying with the reporting requirement. For example, TSA took enforcement action against an agency for not reporting an incident involving a knife, but did not take action against another agency for not reporting similar incidents, despite having been inspected.

On the basis of these findings, in December 2012, we recommended that TSA: (1) Develop and disseminate written guidance for local TSA inspection officials and rail agencies that clarifies the types of incidents that should be reported to the TSOC, and (2) enhance and utilize existing oversight mechanisms at the headquarters level, as intended, to provide management oversight of local compliance inspections and enforcement actions. TSA concurred with both of these recommendations and has taken actions to implement them. Specifically, in September 2013, TSA disseminated written guidance to local TSA inspection officials and passenger and freight rail agencies that provides clarification about the requirements of the rail security incident reporting process. This guidance includes examples and descriptions of the types of incidents that should be reported under the regulatory criteria, as well as details about the type of information that should be included in the incident report provided to the TSOC. Further, as of August 2013, TSA had established an RSI-dashboard report that provides weekly, monthly, and quarterly information about the number of inspection reports that have been reviewed, accepted, and rejected. According to TSA officials, this helps ensure that rail agencies are inspected regularly, by providing the RSI–Ss with greater insight into inspection activities. TSA has also enhanced the utilization of the RSI–Ss by providing them with the ability to review both passenger and freight rail inspections before the inspection reports are finalized and enforcement action is taken. According to TSA officials, this allows the RSI–Ss to ensure that enforcement actions are applied consistently by local TSA inspection officials. TSA also developed a mechanism for tracking the recommendations RSI–Ss make to local TSA inspection officials regarding changes to local compliance inspections, as well as any actions that are taken in response. Collectively, we believe that these changes should allow the RSI–Ss to provide better management oversight of passenger and freight rail regulatory inspections and enforcement actions, though we have not assessed whether they have done so. We also believe these actions, if implemented effectively, will help ensure that the rail security incident reporting process is consistently implemented and enforced, and will address the intent of our recommendations.

TSA Has Taken Steps to Improve the Accuracy and Completeness of Incident Data

In December 2012, we also found that TSA's incident management data system, known as WebEOC, had incomplete information, was prone to data entry errors, and had other limitations that inhibited TSA's ability to search and extract basic information.[20] These weaknesses in WebEOC hindered TSA's ability to use rail security incident data to identify security trends or potential threats. Specifically, at the time of our 2012 report, TSA did not have an established process for ensuring that WebEOC was updated to include information about rail security incidents that had not been properly reported to the TSOC.[21] As a result, of the 18 findings of non-

---

the 19 passenger rail agencies that we included in our review. Ridership data for 2011 were provided by the American Public Transportation Association.

[19] We reviewed inspection data for 19 passenger rail agencies. Three passenger rail agencies had not been inspected, including a major metropolitan rail agency. Local officials we interviewed said it was unlikely that no incidents had occurred at that agency.

[20] GAO–13–20.

[21] TSA could become aware of such an incident through a compliance inspection, media reports, or other Governmental incident management systems.

compliance we reviewed that were a result of failure to report an incident, 13 were never entered into WebEOC, and consequently could not be used by TSA to identify potential security trends. In addition, in December 2012, we found that TSA's guidance for officials responsible for entering incident data was insufficient, a fact that may have contributed to data entry errors in key fields, including the incident type and the mode of transportation (such as mass transit or freight rail). At the time of our report, because of data errors and technical limitations in WebEOC, TSA also could not provide us with basic summary information about the rail security incident data contained in WebEOC, such as the number of incidents reported by incident type (e.g., suspicious item or bomb threat), by a particular rail agency, or the total number of rail security incidents that have been reported to the TSOC.[22] Without the ability to identify this information on the number of incidents by type or the total number of incidents, we concluded that TSA faced challenges determining if patterns or trends exist in the data, as the reporting system was intended to do.

On the basis of these findings, in December 2012 we recommended that TSA: (1) Establish a process for updating WebEOC when incidents that had not previously been reported are discovered through compliance activities, and (2) develop guidance for TSOC officials that includes definitions of data entry options to reduce errors resulting from data-entry problems. TSA concurred with both of these recommendations and has taken actions to implement them. Specifically, in March 2013, TSA established a process for the surface detailee position, discussed earlier in this statement, to update WebEOC when previously unreported incidents are discovered through compliance activities. Additionally, in October 2014, TSA officials reported they have updated the guidance used by TSOC officials responsible for entering incident data into WebEOC to include definitions of incident types. TSA has also made changes to WebEOC that will allow for officials to search for basic information, such as the total number of certain types of incidents, required to facilitate analysis. We have not reevaluated the data contained in WebEOC, but we believe that the changes TSA has made should allow the agency to conduct continuous analysis of the rail security incident data to identify potential trends. We believe these actions address the intent of our recommendations and, if implemented effectively, should improve the accuracy and completeness of the incident data in WebEOC. This should provide TSA with a more comprehensive picture of security incidents as well as allow it to better identify any trends or patterns.

Chairmen Katko and King, Ranking Members Rice and Higgins, and Members of the subcommittees this concludes my prepared statement. I would be happy to respond to any questions you may have at this time.

Mr. KATKO. Thank you, Ms. Grover, for your testimony. We appreciate you taking the time to be here today as well.

Our third witness is Mr. Raymond Diaz, who is currently serving as the director of security at the Metropolitan Transportation Authority. Previously, Mr. Diaz served as chief of the Transit Bureau with the New York City Police Department.

The Chair now recognizes Mr. Diaz to testify.

STATEMENT OF RAYMOND DIAZ, DIRECTOR OF SECURITY, METROPOLITAN TRANSPORTATION AUTHORITY (NEW YORK)

Mr. DIAZ. Good afternoon, Chairman Katko, Chairman King, and other Members of the subcommittees. Thank you for holding this hearing and for inviting me to discuss security at New York's Metropolitan Transportation Authority. Joining me today is Michael Coan, the chief of the department for the MTA Police.

Before joining the MTA in January 2014 as director of security, I served as chief of the New York City Police Department's Transit Bureau, responsible for the safety and security of the MTA, New York's TRANSIT SYSTEM. During my 41-year career with the

[22] To conduct our analysis, we asked TSA to provide all passenger rail incidents reported to the TSOC from January 1, 2011, through June 30, 2012, as well as the total number of incidents reported by selected rail agencies. In response to this request for data, TSA provided us with several inconsistent datasets from WebEOC, which officials attributed to differences in the way the data were searched and compiled from WebEOC.

NYPD, I also served as commanding officer of Patrol Borough North and Patrol Borough South and the School Safety Division. Before joining the NYPD, I served in Vietnam with the United States Marine Corps.

In my present position, I am responsible for the security of the MTA, including coordinating MTA efforts with the Department of Homeland Security, the FBI, the National Guard, the NYPD, and the New York and Connecticut State Police. I oversee the MTA Police Department, which has jurisdiction in 14 counties in New York and Connecticut and patrols a 5,000-square-mile rail network. I am responsible for the implementation and execution of the security strategy that offers maximum protection to the public, the MTA employees, and MTA property.

Before I discuss security in more depth, I would like to set the stage with some basic facts about the MTA. Every day we move more than 8.7 million people on our subways, buses, and commuter rail lines. We are one of the few transit systems in the world that operates 24 hours a day, 7 days a week, 365 days a year. Our 7 bridges and 2 tunnels carry nearly 300 million vehicles a year. Our network of trains, buses, bridges, and tunnels is a trillion-dollar asset, meaning this: If we were to build our network today, including about 9,000 rail cars, 5,000 buses, and millions of other assets, it would cost nearly $1 trillion.

Protecting millions of people a day in a trillion-dollar asset is an enormous task. I can tell you that the MTA's priority is clear: Ensuring the safety and security of our customers and our employees.

To protect our customers and our assets, the MTA employs multi-layered security strategies. Some strategies, like policing, are highly visible. Others are less visible, like structural hardening, advances in technology, and improved communications.

The hallmark of policing our 5,000-square-mile territory is collaboration. Let me explain. In response to the growing threat of active-shooter attacks, over 95 percent of our PD officers have received transit security grant-funded active-shooter training. In addition, over 60 officers have received heavy weapons training. We have a robust See Something, Say Something campaign coupled with security awareness training for our front-line employees. The two serve to encourage vigilance, as well as educate individuals as to what appropriate actions should be taken when suspicious activity is observed. To date, the MTA has trained in excess of 35,000 front-line employees.

The recent incident of a potential active shooter in France thwarted by vigilant rail passengers clearly illustrates the importance of such awareness initiatives and training. Transit Security Grant Program grant awards have also supported our See Something, Say Something campaign and our civilian employee training.

Behind the scenes, one critical layer to us surely is the structural and technological hardening of our infrastructure. Since 9/11, the MTA has invested close to $1.4 billion of local funds towards an aggressive campaign to harden our subway and our commuter rail systems, as well as our bridges, tunnels, and other infrastructure. Critical stations and vulnerable areas have been secured with electronic security systems, consisting of CCTV, intrusion detection,

and access control devices. We have also deployed chemical, biological, radiological detection technology at such locations.

We have benefited from over $400 million in support for our security program from DHS since 2003. TSA and FEMA have helped us immeasurably with grant allocations and reallocations.

Unfortunately, the trend of a shrinking National program has limited our ability to move forward with our capital security mitigations. For example, in fiscal year 2009, the MTA received $92 million of a $349 million National program. Six years later, the National appropriation has dropped by 75 percent, leaving only $87 million for transit agencies across the country.

We are grateful for the support and are pleased that the initial period of performance for transit security grants has been extended to 36 months, which affords us time needed to complete capital security projects funded through the TSGP.

Another layer of MTA's security strategy is communication and intelligence sharing. At the Federal level, we have excellent working relationships with our DHS partners represented by FEMA and TSA. We attend regular meetings, conference calls, and continually exchange information. When potential threats are identified, they are communicated immediately. We share intelligence with many law enforcement agencies on a daily basis through our Inter-Agency Counterterrorism Task Force.

Additionally, we conduct joint patrol initiatives with other regional transportation agencies, including Amtrak, the Port Authority of New York and New Jersey, New Jersey Transit, the New York and Connecticut State Police, the New York State National Guard, and the NYPD. MTA PD detectives represent the MTA on the FBI's Joint Terrorism Task Force, the FBI's Cyber Crimes Unit, the High Intensity Drug Trafficking Area, and the NYPD Counterterrorism and Intelligence Units.

I am proud to oversee this system and its proactive and accomplished security personnel and look forward to continuing to work with my colleagues in law enforcement and you in the House to keep our customers safe and our systems secure. Once again, thank you for inviting me to testify today, and I will be happy to answer any questions.

[The prepared statement of Mr. Diaz follows:]

PREPARED STATEMENT OF RAYMOND DIAZ

SEPTEMBER 17, 2015

Good afternoon Chairmen Katko and King, and other Members of the subcommittees. Thank you for holding this hearing and for inviting me to discuss security at New York's Metropolitan Transportation Authority. Joining me today are Michael Coan, chief of department of the MTA Police.

Before joining the MTA in January 2014 as director of security, I served as chief of the New York City Police Department's Transit Bureau, responsible for the safety and security of the MTA New York City Transit system. During my 41-year career with the NYPD, I also served as commanding officer of Patrol Boroughs Manhattan North and South, and the School Safety Division. Before joining the NYPD, I served in Vietnam with the U.S. Marine Corps.

In my present position, I'm responsible for the security of the MTA, including coordinating MTA efforts with the Department of Homeland Security, the FBI, the National Guard, the NYPD, and the New York and Connecticut State Police. I oversee the MTA Police Department, which has jurisdiction in 14 counties in New York and Connecticut and patrols a 5,000-square-mile rail network. I'm responsible for

the implementation and execution of a security strategy that offers maximum protection to the public, MTA employees, and MTA property.

Before I discuss security in more depth, I'd like to set the stage with some basic facts about the MTA. Every day, we move more than 8.7 million people on our subways, buses, and commuter rail lines. We're one of the few transit systems in the world that operates 24 hours a day, 7 days a week, 365 days a year. Our 7 bridges and 2 tunnels carry nearly 300 million vehicles a year. Our network of trains, buses, bridges, and tunnels is a $1 trillion asset, meaning this: If we were to build our network today—including about 9,000 railcars, 5,000 buses, and millions of other assets—it would cost nearly $1 trillion.

Protecting millions of people a day and a trillion-dollar asset is an enormous task. I can tell you that the MTA's top priority is clear: Ensuring the safety and security of our customers and employees. To protect our customers and our assets, the MTA employs a multi-layered security strategy. Some strategies, like policing, are highly visible; others are less visible, like structural hardening, advances in technology, and improved communications.

The hallmark of policing our 5,000-square-mile territory is collaboration. Let me explain. The NYPD is responsible for patrolling the most heavily-used portion of our network, New York City subways and buses. We work closely with the NYPD to ensure that capital investments are consistent with the latest security and policing strategies.

The MTA PD polices our commuter rail system. Metro-North Railroad and Long Island Rail Road are the two busiest commuter rail agencies in the country. Since 9/11, we've concentrated on counter-terrorism strategies. The department has grown from 494 uniformed officers to 722 today. Fifty K–9 teams are now deployed throughout the system, and we've significantly increased our presence on trains and at stations. In addition to the MTA PD, 721 Bridge and Tunnel officers patrol our 7 bridges and 2 tunnels.

In response to the growing threat of active-shooter attacks, over 95% of our MTA PD officers have received TSGP-funded Active-Shooter Training. In addition, over 60 officers have received heavy weapons training.

We have a robust "See Something, Say Something" campaign, coupled with security awareness training for civilian front-line employees. The two serve to encourage vigilance as well as educate individuals as to what appropriate action should be taken when suspicious activity is observed. To date, the MTA has trained in excess of 35,000 front-line employees.

The recent incident of a potential active shooter in France thwarted by vigilant rail passengers clearly illustrates the importance of such awareness initiatives and training. TSGP grant awards have also supported our "See Something, Say Something" campaign and civilian employee training.

Behind the scenes, one critical layer to our security is the structural and technological hardening of our infrastructure. Since 9/11, the MTA has invested close to $1.4 billion of local funds toward an aggressive campaign to harden our subway and commuter rail systems, as well as bridges, tunnels, and other infrastructure. Critical stations and vulnerable areas have been secured with electronic security systems consisting of CCTV, intrusion detection, and access control devices. We've also deployed chemical, biological, and radiological detection technology at such locations.

We've benefitted from over $400 million in support of our security program from DHS since 2003. TSA and FEMA have helped us immeasurably with grant allocations and reallocations. Unfortunately the trend of a shrinking National program has limited our ability to move forward with our capital security mitigations. For example, in fiscal year 2009 the MTA received $92 million of a $349 million National program. Six years later, the National appropriation has dropped by 75%, leaving only $87 million for transit agencies across the country.

We're grateful for this support, and are pleased that the initial "period of performance" for transit security grants has been extended to 36 months, which affords us the time needed to complete capital security projects funded through the TSGP.

Another layer of the MTA's security strategy is communication and intelligence sharing. At the Federal level, we have an excellent working relationship with our DHS partners, represented by FEMA and TSA. We attend regular meetings and conference calls, and continually exchange information. When potential threats are identified, they are communicated immediately.

We share intelligence with many law enforcement agencies, on a daily basis, through our Inter-Agency Counterterrorism Task Force (ICTF). Additionally, we conduct joint patrol initiatives with other regional transportation agencies including: Amtrak, the Port Authority of New York and New Jersey, New Jersey Transit, the New York and Connecticut State Police, the New York State National Guard, and the NYPD.

MTA PD detectives represent the MTA on the FBI's Joint Terrorism Task Force, the FBI Cyber Crimes Unit, the High-Intensity Drug Trafficking Area program, and the NYPD Counter Terrorism and Intelligence units.

I'm proud to oversee this system and its proactive and accomplished security personnel, and look forward to continuing to work with my colleagues in law enforcement and you in the House to keep our customers safe and our system secure. Once again, thank you for inviting me to testify today. I'm happy to answer any questions you might have.

Mr. KATKO. Thank you, Mr. Diaz, for your testimony and for being here today.

Our fourth witness is Chief Polly Hanson, who serves as Amtrak chief of police, overseeing more than 500 law enforcement officers and civilians across the Nation. Previously, Chief Hanson served for 27 years at the Metro Transit Police, rising to the position of chief of police and director of Office of Law Enforcement and Security at the U.S. Department of Interior.

Ms. Hanson, I will note, and for the rest of the panel, that our votes have been called. So after your testimony, we will take a break to go do the votes and then reconvene.

STATEMENT OF POLLY HANSON, CHIEF OF POLICE, NATIONAL RAILROAD PASSENGER CORPORATION (AMTRAK)

Chief HANSON. Yes, sir. Good afternoon.

The Amtrak Police Department was created to protect Amtrak's employees, passengers, rolling stock, and other critical infrastructure. We do that by working closely with our colleagues in the law enforcement and counterterrorism communities to collect intelligence, pilot new technology, and surge our resources.

The Amtrak Police Department consists of more than 500 members based in 30 locations. Our patrol officers are the most visible part of our department. They patrol stations, ride trains, perform education and enforcement on railroad safety, and are the first response to Amtrak incidents. Our Special Operations Unit consists of officers with tactical skills who perform station surges, conduct random passenger bag screening, perform countersurveillance, and dignitary protection. Our K–9 Program, which consists of both conventional and vapor wake detection dogs, average 1,000 train rides a month.

Terrorist tactics continue to evolve and we must keep pace. U.S.-based extremists will continue to pose the most frequent threat to the U.S. homeland. As tragic attacks in Boston and New York have shown, the new terrorist threat is already here. From lone-wolf attackers to ISIL radicals, we see a greater likelihood of attack now than we have in years.

The internet and cyber space have become the new recruiting ground and the new battle space. Aided by the internet and social media, ISIL has featured plans to kill U.S. soldiers and law enforcement, and the recent attack in France demonstrates the threat is evolving and increasing.

Across the country, we coordinate with numerous other local, State, and Federal agencies. We have officers assigned to the FBI National Joint Terrorism Task Force, as well as joint terrorist task forces in Baltimore, Chicago, New York, Philadelphia, Boston, and Washington, DC.

One of our most visible efforts builds on a partnership with TSA that led to the creation of something called RAILSAFE. Amtrak Police, NYPD, and TSA started RAILSAFE in 2010, and there have been 50 RAILSAFEs in 42 States, the District of Columbia, and Vancouver, British Columbia, involving over 265 agencies and over 1,600 law enforcement members since 2010. Amtrak has used DHS funding to provide our RAILSAFE partners and other first responders with training on the sharing of intelligence and the unified response to Amtrak incidents.

Internationally, Amtrak Police partner with foreign law enforcement agencies in Europe with RAILPOL, where we share information on policing, intelligence, and Amtrak has a working relationship with Interpol. The Amtrak Intelligence Unit coordinates with the United States Department of Transportation. We have members aligned with regional fusion centers. We do welcome the VIPR teams who deploy at many of our stations on an unpredictable and random basis.

Amtrak is a DHS test bed for piloting of new technology, and we have taken advantage of the TSA Baseline for Security Enhancement, which highlights Amtrak's security posture and adherence to accepted security practices.

To extend our reach, we have developed programs that enable our employees, as well as our passengers, to report things that strike them as suspicious. We have trained our employees in techniques to spot suspicious behaviors, and by using phones or texting, have added tens of thousands of eyes to our efforts to watch over our passengers, trains, and facilities. It is a part of our larger strategy of working collaboratively with partner organizations and passengers so that we can add their unique strength to our own to ensure the safety of our systems and the communities we serve.

Amtrak has taken advantage of DHS campaigns like If You See Something, Say Something, and passengers and employees can text us at APD11.

Since the creation of TSA, there have been many security measures implemented. But we need to continue our partnerships, encourage our employees, passengers, and patrons to be observant and report suspicious activity. Thank you for the opportunity to discuss the Amtrak Police role in rail passenger protection, and I look forward to answering any questions you may have when you return.

[The prepared statement of Chief Hanson follows:]

PREPARED STATEMENT OF POLLY HANSON

SEPTEMBER 17, 2015

Chairmen Katko and King, Ranking Members Rice and Higgins, and Members of the subcommittee, good afternoon, and thank you very much for the invitation to testify today. Amtrak takes its responsibility to protect its riders very seriously, and on behalf of Mr. Boardman, our president and CEO, and the men and women of the Amtrak Police Department (APD) I welcome the opportunity to testify before you today.

Amtrak is America's Railroad. Our passengers travel between more than 500 communities in 46 States and our trains operate on over 21,000 miles of track. Amtrak operates more than 300 daily trains delivering over 30 million travelers a year safely to their destinations. The Amtrak Police Department was created to protect Amtrak's employees, passengers, patrons, stations, stops, rolling stock, and other crit-

ical infrastructure. We do that by working closely with our colleagues in the law enforcement and counter-terrorism communities to collect intelligence, pilot new technology, and surge our resources on Amtrak trains, along our right-of-ways, and in our stations and engage our passengers and patrons in being our partners in safety.

The Amtrak Police Department consists of more than 500 members based in 30 locations. While the department was created in the 1970's, it really wasn't until after September 11 that counter-terrorism became a large focus of our security plans. Uniform Patrol Division officers are the most visible part of our department. They patrol stations, ride trains, perform education and enforcement on railroad safety, and are the first response to Amtrak incidents. Our Special Operations Unit consists of officers with tactical skills who perform station surges, conduct random passenger bag screening, and perform counter surveillance, right-of-way patrols, and dignitary protection. Our K–9 program which consists of both conventional and vapor wake detection dogs average 1,000 train rides a month. The Transportation Security Administration (TSA) supports Amtrak's robust K–9 program.

Terrorist tactics continue to evolve, and we must keep pace. U.S.-based extremists will continue to pose the most frequent threat to the U.S. homeland. As the tragic attacks in Boston, Texas, and New York have shown over the last several years, the new terrorist threats are already here. Either alone or in small groups, with the ability to mask the extent of their radicalization, these individuals represent the most lethal of threats. From "lone-wolf" attackers to ISIL radicals, we see a greater likelihood of attack than we have in years. The internet and cyber space has become the new recruiting ground and the new battlespace. Aided by the internet and social media, ISIS has featured plans to kill U.S. soldiers or law enforcement and the recent attacks in France and against tourists in Tunisia demonstrate the threat is increasing.

Across the country, we coordinate with numerous other local, State, and Federal agencies, including the TSA, DHS, NCTC, CBP, DEA, FBI, U.S. MARSHALLS and the U.S. Capitol Police. Amtrak officers are assigned to the FBI National Joint Terrorism Task Force at the National Counter-Terrorism Center, as well as Joint Terrorism Task forces in Baltimore, Chicago, New York, Philadelphia, Boston, and Washington, DC.

One of our most visible efforts builds on a partnership with the TSA that led to the creation of the Regional Alliance Including Local, State, and Federal Efforts (RAILSAFE) Network. More than 200 agencies in over 40 States usually participate in Operation RAILSAFE which increases visibility at stations and stops and along the right-of-way and by water and in the air. Amtrak Police, NYPD, and TSA started RAILSAFE in 2010 and there have been 50 RAILSAFEs in 42 States, the District of Columbia, and Vancouver, Canada involving over 265 agencies and over 1,600 law enforcement members since then.

Amtrak has used DHS funding to provide our RAILSAFE partners and other first responders with training on railroad safety, the sharing of intelligence, and the united response to Amtrak incidents. This training has been provided to almost 300 participants since 2014 in 11 States.

Internationally, Amtrak Police has partnered with foreign rail law enforcement agencies throughout Europe with the RAILPOL organization. Rail policing issues, intelligence, and information sharing are discussed and solid relationships have been established by our participation. Additionally, Amtrak Police has a working relationship with Interpol.

Building on the extensive intelligence, military, and law enforcement backgrounds of its members, the Amtrak Intelligence Unit coordinates with the United States Department of Transportation Office of Intelligence, Security, and Emergency Response and has members aligned with the Washington Regional Threat Analysis Center and the Maryland State Fusion Center. Amtrak Police also welcome the Visible Intermodal Protection and Response (VIPR) Teams who deploy at many of our station facilities on an unpredictable and random basis. On a daily basis, TSA supports Amtrak's random passenger bag inspection program.

Amtrak is a DHS test bed for the piloting of new technology and we have taken advantage of the TSA Surface Transportation Security Inspection Program Baseline Assessment for Security Enhancement, which highlights Amtrak's security posture and adherence to accepted security practices.

To extend our reach, we have developed programs that enable other Amtrak employees as well as our passengers to report on things that strike them as unusual or suspicious. We have trained Amtrak's employees in techniques to spot suspicious behaviors. Using phones or texting, these tools have added tens of thousands of eyes to our efforts to watch over our passengers, trains, and facilities. The ability to leverage our skilled workforce, with its knowledge of the operating environment, is

an important strength that contributes to the security and safety of our system. It is part of our larger strategy of working collaboratively with partner organizations and passengers so that we can add their unique strengths to our own to ensure the safety of our system and the communities it serves.

Amtrak has taken advantage of DHS public awareness campaigns like "If You See Something, Say Something" and texting a tip to APD11 which was another initiative supported by DHS funding. I want to emphasize that since the creation of TSA there have been many security measures implemented but we need to continue our partnerships, encourage our employees, passengers, and patrons to be observant and report suspicious activity or behavior.

Thank you again, for this opportunity to discuss the Amtrak Police role in rail passenger and infrastructure protection. I look forward to answering any questions that you may have.

Mr. KATKO. Thank you, Ms. Hanson.

There is a series of three votes. We anticipate it being—the first vote is just about ready to be expired. So we have got to roll. We have two 5-minute votes after that. As soon as the last vote is done, we will start here again in 10 minutes. So without objection, the committee and subcommittee is in recess subject to the call of the chair.

[Recess.]

Mr. KATKO. The Subcommittees on Transportation Security and Counterterrorism and Intelligence will come to order. I now recognize myself for 5 minutes to ask questions.

I want to make kind-of an overarching observation first before I get into some questions, and that is I am very mindful of the surface transportation attacks that have occurred overseas in Europe, the tragedy of them from years ago until more recently and the attempts more recently. It does make me conclude that we are vulnerable to that in this country as well.

It was compounded when I went to Penn Station recently and took a tour there, and just the sheer mass of people there on a regular basis, and the different entry points and the different trains that are there, the different agencies that are there, Amtrak and Metro-North, and the subways and everything else. It just really does, I shudder to think what a tragedy that could happen there, just like you think about in airports.

The difference between the rails and airports are that airports have a tremendous amount of scrutiny to them right now and a tremendous amount of security. I am concerned that the surface transportation system is lacking in the amount of security that it needs. But I am interested to hear from the viewpoints of all of you that are on the front lines every day, particularly Mr. Diaz and Ms. Hanson and Mr. Mayenschein. Also your observations, Ms. Grover, throughout your testimony with others today, as to what you think can be done better.

So I guess to start out with Mr. Diaz and Ms. Hanson, since you have been on the front lines for most of your careers, if not all of them, that you kind-of give me your observation of what you think the overall state of security is and what you think needs to be done moving forward. We can start with Ms. Hanson, if you would please.

Chief HANSON. I think there are a couple really wonderful things working. You mentioned New York. I can speak to there, but other places as well. In my testimony and others, you did hear people talk about collaboration and partnership.

So New York has a very strong partnership with all the entities and more that you described that do provide service in and out of Penn Station. They, law enforcement executives, security people, freight members, and others have quarterly meetings and just have had several to coordinate and communicate about the Pope's visit.

So I think you have a very strong presence there that is integrated, a tremendous amount of professionalism. That said, you also have layered security in the way that there is technology. Certainly using things like text-a-tip, which we use and other transportation entities use, because you do have to rely on the 700,000 people that are in Penn Station a day and the thousands of employees that we all have there.

In my 27 years at Metro, I always thought one of the most important employees was the custodian, because that is somebody who is very familiar with the station and knows when something is suspicious.

So we do have layered protection with biological detection. Some places use chemical detection. Long guns are deployed. You have countersurveillance, and by that I mean members that are not in uniform that have been trained to look for suspicious activity. Then I think the strong intelligence sharing that we have that may involve Federal partners and may not. The group that is in partnership in New York have each other on speed dial and text. The chief texted me when we had the derailment in Philadelphia to see if I needed any resources or support. Of course, in an event like the one we had in Philadelphia, the first inquiry is always, is there an act of terrorism?

I can speak to what happened Friday at Union Station, which was not an active-shooter situation but did involve a shooting. We had done quite a bit of training with our employees, our business owners, our property manager, and our passengers. People did what we had taught them to do. Our businesses locked the doors, turned off the lights, and hid. Our employees hunkered down, in some cases in the back in the track area where they took passengers. We had an Acela that was loading. Our crews got on there, locked everybody down on that train.

We had a response from the region because we were surging that day, but we had a coordinated response, and within 14 minutes, we had train service back up because of the way that event was mitigated, the way things were communicated, and the strong partnerships that we have.

I think you alluded to the fact that something did happen in 1993 on the Long Island Railroad, 6 people were killed and almost 20 people were injured by somebody, in that case, was mentally ill but still came on the train with a gun. An off-duty Long Island Railroad police officer was the one that made the lock up. But in that case, much like France, the passengers on that train jumped on that guy and subdued him.

So I think it is a combination of factors with law enforcement, our partnerships, the training we provide our employees, and the intelligence that we share as a community.

Did I answer your question, sir?

Mr. KATKO. Yes. We could be here all day really discussing it. It is unfair to ask you to summarize it so quickly, but that is the time we have.

Just in my time left, Mr. Diaz, if you could briefly respond to my question?

Mr. DIAZ. Chairman, I think as of September 2014, at the Governor's direction, if you look at Penn Station and some of our major terminals, like Grand Central, we substantially increased, by probably about 40 percent on the MTA PD side, increased our police presence there, our uniformed presence. In addition to that, the National Guard, New York National Guard was substantially increased in our terminals. The New York State Police now also are present in both of our terminals, Penn Station and Grand Central Station, in addition to riding our trains.

So I feel very comfortable with the level of uniformed presence we have in those terminals. However, there is a concern because we were able to support that through transit security grant funding and a large part of that funding expired August 31. We have sort-of, like, we are running out of money.

We thought we would probably have to cut back a little bit, but the direction from our Governor's office was that he did not want to see an increase. So we have been spending a lot of money to put those extra resources there. That is a concern of mine, at some point, that we are not going to have the funds to continue the level of presence we have had in those terminals.

Mr. KATKO. Thank you, Mr. Diaz.

Of course, I have a thousand more questions I could ask, but I am going to respect the clock here as best I can. The Chair now recognizes the Ranking Minority Member of the subcommittee, the gentlelady from New York, Miss Rice, for any questions she may have.

Miss RICE. Thank you, Mr. Chairman.

Mr. Diaz, I just want to start with you, Mr. Diaz. The New York subway system, I would say, arguably, right, is considered larger than most of those, any other passenger rail systems in terms of passengers per day. How many people, what is the number, 8 million?

Mr. DIAZ. It is about 6 million passengers a day. We run over about 7,800 trains on a week day.

Miss RICE. So how do you run such a vast operation and do it as successfully as you have? Now, taking into consideration the fact that, obviously, money is a big priority, and we hear you loud and clear about funds drying up making it more challenging for you to do your job. But you do it pretty well. I mean, I ride the subway, and I am pretty amazed that is done. I mean, you have issues. But how do you get it right? The report that Ms. Grover did: What, if any, improvements would you make if you could?

Mr. DIAZ. Well, what I would like to say, the New York City Police Department actually patrols our transit system. They have about 2,600 officers and they do a fantastic job. I mean, crime is like a minimum number of crime. We average about, I think, six crimes a day for that entire transportation system.

They do a fantastic job of patrolling it. We have surge operations. We have bag inspections. Robust K–9 units that patrol those areas.

We have a pretty elaborate CCTV and electronic security systems. Intrusion detection. Our tunnels are hardened to make it difficult for anybody to get into our tunnels and do anything to our trains and to our infrastructure.

We have a lot of infrastructure protection in addition to the railroads. We have, it was mentioned earlier, Penn Station, if you look at Penn Station, it has bollards that circle almost the entire station. So if someone with a large bomb in a large vehicle, they are not going to get into that station. So we feel very comfortable with that.

But those are the types of things that we like to do to protect our system. Again, it takes money to do that.

Miss RICE. So you describe a very good relationship, obviously, with the NYPD. My question would be to Ms. Hanson, to you, again, Mr. Diaz, and Mr. Mayenschein, the Chairman said in his opening statement that up to this point a lot of the focus, at least before the incident that happened in Paris or outside of Paris, a lot of the focus in terms of security and transportation security has been on the aviation industry.

So what I would like you to talk about, the three of you, is what level of cooperation and coordination do you have with people who are focused on that area, aviation security, and land and surface security? Because there is a lot of overlap there. So however you want to take the answer.

Mr. DIAZ. I can just say, on the intelligence side and information sharing, like recently there were some threats to aviation, we get immediate notifications for our partners at TSA. We have excellent communication when it comes to intelligence, I think. I am very impressed.

I mean, every day I get intelligence information from all of our law enforcement partners, our Governmental partners. I have an interagency counterterrorism task force that every day gets briefings from all of those other areas and puts together a nice briefing package. We get that before 7 o'clock every morning. We distribute that to other law enforcement agencies.

The information sharing, I think, is really outstanding. We have officers embedded into JTTF, New York City Intel-CounterTerrorism. The information sharing, I think, is outstanding. I don't think there is any problem with that.

TSOC, I know, was mentioned. About an hour ago, I just saw a TSOC notification from our New York City Transit to TSOC regarding a fare evader that didn't pay a fare and had a firearm on him illegally.

So I think we have come a long way.

Miss RICE. Mr. Mayenschein—because I have one question I want to ask all of you—would you agree, and Ms. Hanson, would you agree with Mr. Diaz's assessment?

Mr. MAYENSCHEIN. Absolutely. I think what has happened with the surface transportation system is almost magical. It is a perfect match of Government and the private sector coordinating instantaneously and sharing information back and forth.

This is all pretty much in absence of regulations. Aviation, maritime is heavily regulated. Not so, so much in surface. This has all been done because of the need to do it. This constant sharing back

and forth is really quite tremendous. We make each other better. They improve what we do. We improve what they do. We share the best practices across the networks. When we get information from GAO about improvements that need to be made, we welcome those and make those improvements. We just continually get better. It is pretty amazing to me.

Miss RICE. Ms. Hanson, would you add anything to that?

Chief HANSON. Yes, two things. The Federal security directors out at the airports, we do have a close relationship with them at Amtrak because we do get resources from them. So there is regular dialogue.

The other thing that I would say, which was a point that you have made, so aviation, and this isn't just recently, since September 11, the focus has really been on aviation. Of course, aviation moves millions of people a year, and mass transit moves billions, but the funding has been the reverse. So the money is focused on aviation versus transportation.

I would ditto my colleague here where, because of the appropriations, the 2015 money has been delayed. We do rely on that money for additional resources for events that we will have, such as the Pope, in our case, the Super Bowls, and events like that where we have an increased threat because of the increased ridership.

So the funding that we have gotten from the intercity passenger grant and that they have gotten from the transit security grant is something we have really come to rely on and is what has allowed MTA to do the infrastructure that they have done and the campaigns and some of the intelligence sharing. So that would be dramatic for us to have a reduction in funding.

Miss RICE. Message received. Well done.

One last question. In 5 words or the less, what is the biggest threat to our surface transportation system?

Mr. MAYENSCHEIN. Certainly the unknown, the home-grown, unknown, violent extremist. They are like an unguided missile, like a scud missile. We just don't know that they are there. I think that is the biggest threat.

Ms. GROVER. The fact that the systems are just wide open.

Chief HANSON. It has been explosives. It will be explosives. Then the lone wolf is a serious consideration, because somebody with a weapon, we see what they can do, and somebody with a knife, we see what they can do. But it is the combination of lone wolf and explosives.

Mr. DIAZ. I concur.

Miss RICE. Great. Thank you all.

Mr. Chairman, I just ask unanimous consent that Mr. Langevin be allowed to sit and question the witnesses during this hearing.

Mr. KATKO. Without objection, so ordered.

The Chair now recognizes the Chairman of the Subcommittee on Counterterrorism and Intelligence, the esteemed gentleman from New York, Mr. King, for any questions he may have. He told me to say "esteemed" by the way.

Mr. KING. It was supposed to be "very esteemed." In any event, thank you, Mr. Chairman.

At the outset let me just say that, as Miss Rice said, the message is received. I really have to make sure that we deliver that to peo-

ple in my party who play games with the spending and don't realize there is consequences. Any talk of Government shutdown, of money not coming, even if it comes months from now, the damage can be done. So your message is well received certainly by me.

I have two questions, and it will be to Mr. Diaz and to Chief Hanson. First of all, thank you both for your testimony, and all of you for your testimony, and to you two in law enforcement, for the work you have done over the years.

Two questions. Taking Penn Station and Grand Central, where everything comes together, you have the New York City subway system, you have Metro-North, you have Amtrak, how well-constituted are you as far as incident command? Who is in charge when something occurs? Is that delineated as to who is responsible when an incident occurs? Also, does the FDNY get involved in that? Because here you have, let's see, at least three, four police departments, you have the National Guard. Again, I am just wondering, is that all coordinated as to who is in charge and who is not?

Second on that, going back to years ago with the Transit Police, there was the problem with communications. How are the communications, the radio communications between the various police departments at Penn Station and Grand Central? That is probably the one area where all of you come together. Either one. Mr. Diaz, you can go first.

Mr. DIAZ. Yes, Chairman. Incident command, again, Grand Central is a Metro-North property. We do have also New York City Transit presence in Grand Central. We have great a relationship with them, a great working relationship. There is a fire brigade assigned to Grand Central that works for Metro-North, and they have a great relationship with the fire department, all the fire department chiefs.

I think as far as interoperability, I think we get along very good. As far as radio communication, that might be a little more difficult, but I think more important than radio communication, I think, is interagency cooperation and interagency interaction with each other. I think that we get the job done.

Chief HANSON. I would say at Penn Station, very similar. We have a very strong emergency manager there. People know where to come. There are regular exercises——

Mr. KING. Emergency manager, is he with Amtrak?

Chief HANSON. He is, yes, sir. Retired NYPD and has a very close relationship with the fire department. Everyone knows where to come. They regularly exercise. Unfortunately, there are enough events, smoke in a tunnel, that people do have an opportunity to exercise those capabilities.

I think interoperability will always be an issue. Even with our potential access to 800 megahertz, it is not so much just being on the frequency, it is the other back end, cabling in a tunnel and some of the infrastructure that is so old.

But I think we have very strong relationships, very strong incident and unified command.

I would want to go back to one of your points about funding, and I am not belaboring it——

Mr. KING. Go ahead.

Chief HANSON [continuing]. But sequestration did impact us very negatively. In our case, it diminished our grants by half a million dollars and it set us back over a year for our K–9 Program with TSA. So we have one person in TSA K–9 training now, and if the Government shuts down, I would imagine that they have to come back home. We have two more dog handlers going to Lackland Air Force Base in October, and I would imagine if there is a shutdown, they have to come down.

So it has taken us a year to catch up because of sequestration. Now, when we are trying to build our K–9 program back up, we will be limited by what happens here.

Mr. KING. One final question. Is everyone allowed to partake in table-top exercises as far as the police departments?

Mr. DIAZ. [Inaudible.]

Chief HANSON. I think what you heard earlier in the testimony from TSA was, at Amtrak's request, TSA sponsored an I–STEP tabletop in Philadelphia. It was for all first responders and Federal, local, State entities, and it was the first table-top, and it was very effective, very well received.

Mr. KING. Thank you all for your testimony and your service.

I yield back.

Mr. KATKO. Thank you, Mr. King.

The Chair now recognizes the Ranking Minority Member of the Subcommittee on Counterterrorism and Intelligence, the gentleman from New York, Mr. Higgins, for any questions he may have.

Mr. HIGGINS. Thank you, Mr. Chairman.

First, just let me thank you, because a lot of what you do is about what didn't happen. You rarely get credit for what didn't happen. So thanks for all you have done to keep things from happening.

Lawrence Wright wrote a book called "The Looming Tower," which is a Pulitzer Prize-winning book about 9/11, and in it, he recounts the experience of an FBI agent working in his office in New York City. When the second plane hit the South Tower, he physically got sick because he knew that between the FBI, the CIA, and other law enforcement agencies, that they had the intelligence to perhaps thwart that attack on New York City and the Nation.

So the sharing of information was very, very important, from which the PATRIOT Act came. A lot of things were added on to it that were objectionable to people, but the bottom line, the original thrust was to remove the barriers that existed between various law enforcement agencies so that they could pool their resources, they could share information, toward the goal of more effectively stopping terrorist activity.

Mr. Diaz, New York City is probably, you know, all of its law enforcement agencies, all of the affiliates, is probably the greatest counterterrorism organization in the world—not out of choice, but out of necessity. You touched on it a little bit, but you had also mentioned that there are 6 million people that travel on those trains every day in 78 different trains. Can you talk a little bit more about how that information is shared? Is that a result of policy or the result of just the intuitive relationship that exists between law enforcement agencies towards the same goal, and that is protecting your common constituency?

Mr. DIAZ. Yes, sir. I think we all have the same goal. Again, like I said earlier, we have detectives that are assigned to JTTF, that are assigned to HITDA, that are assigned to NYPD Counterterrorism, and NYPD Intelligence. There is great information sharing. I mean, we talk together all of the time. Every day I receive briefings and alerts.

I can say that, and it is funny, because it is not just at working hours. We have such a great relationship. We have fraternal organizations and we see each other at evening, at dinners, and other places. So we are constantly talking to each other. I think we have come a long, long ways from 9/11, and I don't think those issues that existed then exist anymore today.

Mr. HIGGINS. So I presume that that is driven in large part by just an inherent sense that New York City is always going to be a major target, it is a high-impact target, and, thus, the role of law enforcement agencies working together is probably, while it is important generally, it seems to be particularly important in a city like New York.

Chief HANSON. Well, I would say a couple of things to that. Amtrak has assigned somebody to the National Terrorism Task Force, so that we have the overarching, because we are in 46 States.

One of the things that I would highlight, though, is after September 11, then-Amtrak Police Chief Sonja Proctor established a group called the Northeast Corridor Coalition. So that group starts in the District of Columbia and goes to New York City. Regularly there is an intelligence component to that and then there is the higher-level executives, to include myself, Chief Bratton, and the chiefs in every town, State, from the District of Colubia to New York. Tremendous amount of exposure, for some people, who the first time we road the train didn't even know Amtrak went through their city.

So that has allowed a growth of information sharing, relationships, a real sensitivity that people don't always have towards transportation policing. Transportation policing is very different and defined and specific. That is why that community of folks that are very similarly situated with those responsibilities is so important for those groups to share information.

Mr. HIGGINS. Thank you very much. I have no further questions. I yield back.

Mr. KATKO. Thank you, Mr. Higgins.

The Chair now recognizes the gentleman from Texas, Mr. Ratcliffe.

Mr. RATCLIFFE. Thank you, Chairman Katko and Chairman King both, for holding this hearing.

The terrorist attacks of September 11 certainly showed the entire Nation that terrorists are willing to go to virtually any length and any means to inflict harm on the American people. In the years after September 11, the Federal Government has certainly taken a number of necessary steps to secure our airports and our airplanes from future attacks.

But, as we all know, terrorists don't operate under conventional rules. I know this well as a former terrorism prosecutor. Terrorists adapt and they find new methods to exploit security and

vulnerabilities to achieve their goal of mass casualties. So we have seen that in, frankly, places around the world.

The district that I represent, the Fourth Congressional District of Texas, is full of small towns, like many of those that span this entire country. Almost all those communities have a bus stop and a train stop, whereas, they may not have an airport. So I would like to start with you, Ms. Hanson. Do you happen to know how many commercially-operated passenger air traffic hubs there are in the United States?

Chief HANSON. I flunk.

Mr. RATCLIFFE. I understand it might be a better question for Mr. Mayenschein. I think it is around 200. The reason I ask is, by comparison, how many Amtrak stations are there around the country?

Chief HANSON. Well, we go to 500 destinations. What I would like to tell you is that in small towns that you talked about, we took DHS money to train our partners in those small towns who we are very reliant on. We have regional detectives. But some of the response time, depending on where they are in relation to the train, could be an hour, 2 hours.

So we have had those detectives cultivate close relationships with local law enforcement. The RAILSAFE Program that we described is an output of that. So we call on those folks during particular times to work with us and other partners to increase visibility.

What I did was take DHS money to create a day-and-a-half course that, first of all, identifies what the threat is in the transportation environment. It explains how Amtrak collects intelligence and shares it. Then we run through a table-top exercise, one for a suspicious package and one for an active shooter. We have done that starting in 2015 and trained hundreds of law enforcement folks in 11 States.

Mr. RATCLIFFE. Okay. But in terms of response time and some of what you related, that is important, but before we get there, I guess, my concern is what we have seen in Europe, and I have intimated before that we have seen a number of surface transportation terrorist attacks. Last week I was at Union Station, took an Amtrak train, and I didn't go through security at all when I got on that train like I do at an airport. So other than the things that you just related——

Chief HANSON. You may not have thought you went through security. We have a very robust vapor wake detection program. So those dogs that you see walking around there that look so nice with the floppy ears and they are very animated and excited were possibly smelling your wake to see if you had explosives.

We also, as I mentioned earlier, have tactical units that are doing countersurveillance. So they are observing people's behavior. We also have people on trains and other capabilities. So you may not have seen the security. It doesn't mean that it is not there.

Unfortunately, last year we had an attack on a train in Niles, Michigan. There we do not have the resources. They attacked our conductor, hurt him very bad. It was an emotionally disturbed man. We had to rely on the Niles Police Department who came and

mitigated that situation. So it was a coordination of our efforts with our local law enforcement colleagues to respond.

Mr. RATCLIFFE. Okay. Well, and as I related, I didn't go through a formal security checkpoint or clearance like you see at the airport. One of the other things was that neither did my luggage that was with me and I didn't see that. On trains you see different sizes, everything from large suitcases to backpacks.

Other than dogs and walking patrols, are there any mechanisms in place for the inspection of luggage?

Chief HANSON. Amtrak is going to start a program starting October 1 where there is going to be restrictions imposed on the size and number of luggage. As a result of that, there may be more observation about luggage. But no, we are not screening your luggage like an airline does.

Mr. RATCLIFFE. Well, I see my 5 minutes went very quickly, so I yield back.

Mr. KATKO. Thank you, Mr. Ratcliffe.

The Chair now recognizes the gentleman from New Jersey Mr. Payne.

Mr. PAYNE. Thank you, Mr. Chairman, and to our Ranking Member.

According to the rail industry officials, the transport of crude oil on trains through dense urban areas has increased 40-fold since 2008. In addition to that, over the past decade or so railroads have begun shipping large quantities of flammable liquids, such as ethanol and crude oil, creating an entirely new response challenge.

Every day, dangerous rail freight carrying security-sensitive cargo travels throughout my district, weaving through residential areas and passing by schools and homes and businesses. In fact, Bakken crude, the more flammable oil, which makes it probably the most dangerous to transport, travels along New Jersey's rail line at a volume of 15 to 30 million gallons per day.

I have said it before in the whole committee and in my subcommittees and I will say it again, my district has the two most dangerous miles in America for terrorist targets, and that is in the area around Newark, New Jersey, and Elizabeth, where the rail, the interstate, the airport, the port, and chemical installations are within a 2-mile radius.

With that said, Mr. Mayenschein—did I get it right?

Mr. MAYENSCHEIN. Yes.

Mr. PAYNE [continuing]. What role does TSA playing ensuring that dangerous rail freight in the communities that they must travel through are secure as can be? I have put forth legislation in order to strengthen the rail cars that carry this dangerous oil. So to my question?

Mr. MAYENSCHEIN. So there are a couple levels here. First of all, this Rail Sensitive Security Material, the RSSM, is something that we do pay attention to, that is regulated. It is inspected. There are regulations that require inspections for certain things. So that is your toxic inhalation hazards, your liquefied chlorine, all the methylethanol bad stuff that is on trains. But that is not Bakken crude. That is a hazardous material, a different classification. There are regulations requiring hazardous material.

So with the rate of inspections that go with this RSSM material, when it is transferred from shippers there are required inspections, when it transfers from one company's rail car to another company's rail car, there are required inspections, a surveillance of paperwork, and that sort-of thing.

Mr. PAYNE. As we have seen over the past several years, the major explosion in Canada, we had an incident in Lynchburg, Virginia, and also a situation where a train derailed and fell into the James River in Virginia. I am very concerned about those issues.

So how does TSA track the trains carrying the hazardous material in real time? Are there any steps taken en route from trains in high-threat urban areas? Mind you, my other issue is when these cars are sitting railside, the security of that is in place, it seems very lacking when it is just sitting in the yard to move to its next destination.

Mr. MAYENSCHEIN. So if there is RSSM, there is toxic stuff, the car needs to be attended. I mean, that is part of the requirement, it needs to be attended.

Mr. PAYNE. We are finding that that is not the case, though, to the degree that we feel that it is necessary in order to secure that.

Mr. MAYENSCHEIN. Okay, I will take that back and take a look at that for you and get back to you specifically and get you very specific data, particularly for the Newark area.

To the other part of your question, the TSA doesn't currently track hazardous materials in real time. So we don't presently do that. The TSA does have regulation and procedures in place to locate shipments of rail security and sensitive materials in the event of an elevated threat condition. So if there is an elevated threat condition, we will immediately reach out to the partners, the railroads, and they have 30 minutes to respond back to us to identify where those toxic inhalation hazards, those RSSM materials are located.

Mr. PAYNE. Okay.

Mr. Chair, I will yield back.

Mr. KATKO. Thank you, Mr. Payne.

The Chair recognizes the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

I want to thank our witnesses here today.

If I could, I would like to change tack a bit and ask about another threat that is facing our surface transportation system, and that is relating to cyber attack. So, Mr. Mayenschein, can you just give us a brief overview of TSA's actions in this domain?

Mr. MAYENSCHEIN. Well, we are just now develop—we have always had an eye on cybersecurity, but in the last year this has become something that we are paying great attention to. Particularly we have seen a denial-of-service attacks at airlines, possibly other attacks.

So we are connected through the interagency. We are talking to our partners out in the private sector about cybersecurity. We address it. Just recently we had a newsletter that went out to our surface partners and right on the front page was cybersecurity.

So we are on top of it. We are learning, like everyone else is. This is another new threat against our homeland.

Mr. LANGEVIN. I think it is important, especially when you look at things like skid attacks. The same type of system that governs pumps and balances is the same thing that governs the switches and such to keep trains on track or to change track and such and could obviously be potentially penetrated.

Can you also describe TSA's role in developing guidance for the transportation sector as it relates to the NIST Cyber Framework?

Mr. MAYENSCHEIN. Well, again, we are connected through all the agencies. In my shop at the TSA, I am the NIST builder for the TSA. So I am the direct connection there. It is a vibrant, on-going process. You know, I would be welcome to come and talk to you about how we do that very specifically. It is very convoluted, complex, but there is some great work that is done there.

Mr. LANGEVIN. Sure. I would like to do some follow-up on that then.

Mr. MAYENSCHEIN. That is great.

Mr. LANGEVIN. Mr. Diaz, Ms. Hanson, can you describe how you view the cybersecurity risk to your respective organizations? How do you go about making risk-management decisions? Do you feel that you have adequate in-house resources of information security? Whom do you partner with to help protect your assets?

Mr. DIAZ. On the MTA PD side, we have a lieutenant and two investigators that are assigned to the FBI Cyber Task Force. I think we have gotten a little ahead of the curve on that because we haven't had any real issues.

But our IT department is ahead of the curve on that. They have a number of things in place. I am not really a computer expert, but I know that we get probes every single day, numerous probes into our system, and they have all been defeated. But it is a concern, and we do have our personnel assigned with the FBI so when that event comes we have things in place that are ready to address it.

Mr. LANGEVIN. Ms. Hanson.

Chief HANSON. Amtrak used DHS funding to have a vulnerability risk assessment done. Our IT section, which is not in the police department, has increased their personnel and staffing. We closely align and have a very close relationship with the FBI.

The FBI did recently put out some areas that they thought needed attention because of some of the threats from ISIL for September 11, and because of that they have got outsourced young hackers who work with our IT team, security team, to make sure that we are aware of who is trying to probe our system.

We obviously have other concerns as a result of some of the new train sets we are building to make sure that we have and continue to work with the FBI about concerns there that could be in place to gather information that would be inadvertent and unintentional, but have a bad consequence.

Mr. LANGEVIN. Thank you.

Mr. Mayenschein, going back to you again, how does TSA handle reports of cybersecurity intrusions and events? Do they count as security incidents? Are they reported to the TSOC and entered into the WebEOC system? Does TSA have any additional steps it takes for cyber incidents as compared to more traditional security events?

Mr. MAYENSCHEIN. Well, again, we are just now building through a couple different departments at the TSA a coalition inside the

TSA to start paying attention to these, not that we haven't been paying attention to them.

I don't know specifically if this is a reported event. I will get back to you specifically if cyber events or cyber attacks are reportable to the TSOC.

Certainly they should be and I will require that. That is something that I can do. If they are not, the———

Mr. LANGEVIN. I would also like to know what happens once the cyber incident is reported, what is the follow-up? How do you ensure that the vulnerability is closed?

Mr. MAYENSCHEIN. Well, again, if it is internal to the TSA, and I don't know of any of those events, but if it is something to one of our security partners that happened in the private sector, there is again this great dialogue and communication to kind-of close those things. But in additional steps, we will make sure that everybody within our stakeholders would know, this sharing of information, that there was an attack, cyber attack, and how it was done, and we would share that immediately.

Mr. LANGEVIN. Ms. Grover, do you have anything to add?

Ms. GROVER. Well, just that 1 of the 10 categories of incidents that is required to be reported to the TSOC is the general category of threats. So it would depend on the specific guidance that TSA had developed about how to define threats about whether or not those are reported.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Mr. KATKO. Thank you, Mr. Langevin.

Before we conclude, there are a couple of overarching observations that I want to make. No. 1 is that, when I was at the 9/11 museum last Monday, September 8, for our field hearing, there was much discussion about the fact that people forget about 9/11 outside of New York City because they think that the terrorist threat is just focused on New York City. I know much of our testimony today was about New York City.

But it is pretty clear to me and it is pretty clear to the committee that a terrorist threat is Nation-wide, and we can't stress enough the importance of having a discussion about Nation-wide threats. We have had a lot of discussion about New York and a little bit about Washington, but it is a Nation-wide threat, and I know you are all aware of that. But I just want the public to understand that it is not limited to New York City by any stretch of the imagination. The recent lone-wolf attacks we have seen in Chattanooga and elsewhere bear that out.

So it is a concern going forward that the diligence and the competence and the professionalism that is displayed in the major urban areas needs to be branched out to the other areas. It is a discussion we need to continue to have. I know with the resources the way they are, that is a major concern. So I am sure we will have more discussions about that going forward.

The other thing is, Ms. Grover, you didn't have a lot of opportunity to speak today, and some people are relieved with that and some people are not when you are a witness. But I will tell you that your reports are always extremely well done and we do read them and we do digest them and we do learn from them. So please keep up the good work that you are doing. Appreciate it.

Ms. GROVER. Thank you, sir.

Mr. KATKO. All right.

Now, I thank the witnesses, all of you, for your testimony, and the Members for their questions. The Members of the committee may have some additional questions for the witnesses, and we will ask you to respond to these in writing. Pursuant to Committee Rule 7(e), the hearing record will be held open for 10 days.

Without objection, the subcommittees stand adjourned.

[Whereupon, at 4:12 p.m., the subcommittees were adjourned.]