SECURING OUR SURFACE TRANSPORTATION SYSTEMS: EXAMINING THE DEPARTMENT OF HOMELAND SECURITY'S ROLE IN SURFACE TRANSPORTATION TECHNOLOGIES

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION AND PROTECTIVE SECURITY

AND THE

SUBCOMMITTEE ON EMERGENCY PREPAREDNESS, RESPONSE, AND COMMUNICATIONS

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JANUARY 30, 2018

Serial No. 115–47

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE

30–193 PDF WASHINGTON : 2018

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
JEFF DUNCAN, South Carolina
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
JOHN KATKO, New York
WILL HURD, Texas
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
MIKE GALLAGHER, Wisconsin
CLAY HIGGINS, Louisiana
JOHN H. RUTHERFORD, Florida
THOMAS A. GARRETT, JR., Virginia
BRIAN K. FITZPATRICK, Pennsylvania
RON ESTES, Kansas
DON BACON, Nebraska
BENNIE G. THOMPSON, Mississippi
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
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
J. LUIS CORREA, California
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California

BRENDAN P. SHIELDS, *Staff Director*
STEVEN S. GIAIER, *General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
HOPE GOINS, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION AND PROTECTIVE SECURITY

JOHN KATKO, New York, *Chairman*

MIKE ROGERS, Alabama
CLAY HIGGINS, Louisiana
BRIAN K. FITZPATRICK, Pennsylvania
RON ESTES, Kansas
MICHAEL T. MCCAUL, Texas *(ex officio)*
BONNIE WATSON COLEMAN, New Jersey
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
BENNIE G. THOMPSON, Mississippi *(ex officio)*

KYLE D. KLEIN, *Subcommittee Staff Director*

SUBCOMMITTEE ON EMERGENCY PREPAREDNESS, RESPONSE, AND COMMUNICATIONS

DANIEL M. DONOVAN, JR., New York, *Chairman*

PETER T. KING, New York
MARTHA MCSALLY, Arizona
JOHN H. RUTHERFORD, Florida
THOMAS A. GARRETT, JR., Virginia
MICHAEL T. MCCAUL, Texas *(ex officio)*
DONALD M. PAYNE, JR., New Jersey
JAMES R. LANGEVIN, Rhode Island
BONNIE WATSON COLEMAN, New Jersey
BENNIE G. THOMPSON, Mississippi *(ex officio)*

KERRY A. KINIRONS, *Subcommittee Staff Director*
MOIRA BERGIN, *Minority Subcommittee Staff Director/Counsel*

CONTENTS

Page

FOR THE RECORD

SECURING OUR SURFACE TRANSPORTATION SYSTEMS: EXAMINING THE DEPARTMENT OF HOMELAND SECURITY'S ROLE IN SURFACE TRANSPORTATION TECHNOLOGIES

Tuesday, January 30, 2018

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON TRANSPORTATION AND
PROTECTIVE SECURITY, AND
SUBCOMMITTEE ON EMERGENCY PREPAREDNESS,
RESPONSE, AND COMMUNICATIONS,
WASHINGTON, DC.

The subcommittees met, pursuant to notice, at 2 p.m., in room HVC–210, Capitol Visitor Center, Hon. John Katko (Chairman of the subcommittee) presiding.

Present: Representatives Katko, Donovan, Higgins, Rutherford, Estes, Watson Coleman, Payne, Keating, and Langevin.

Mr. KATKO. The Committee on Homeland Security, Subcommittee on Transportation and Protective Security and Subcommittee on Emergency Preparedness, Response, and Communications will come to order. The subcommittees are meeting today to examine the degree to which the Department of Homeland Security leverages its research and development expertise to improve the security architecture of our Nation's surface transportation systems. Specifically, the subcommittees will examine how the TSA and the Science and Technology Directorate collaborate to improve security capabilities and address identified needs.

I now recognize myself for an opening statement.

The free movement of goods and people depends on the security of our transportation networks. A substantial number of Americans utilize surface transportation on a daily basis, including over 10 billion riders annually on 6,800 U.S. mass transit systems.

While TSA is responsible for securing all of America's transportation systems, its approaches to aviation security and surface transportation security are, to say the least, markedly different. Whereas TSA is directly involved in security operations at airports, the agency provides oversight and assistance to surface transportation modes through partnerships with operators as well as State and local authorities. This collaborative, whole-of-the-community approach helps make sure that resources are applied efficiently and have the highest efficacy in reducing risk to the Nation's transportation systems.

We know that DHS provides support through security threat assessments, explosives detection canines—nowhere near enough—and security grants. However, our subcommittees hope to learn more today of how S&T—short for Science and Technology—and TSA are helping to drive security technology innovation for the surface sector.

This committee understands that this is a complex undertaking, and I hope we can help you with this critically important responsibility. The current threat environment facing surface transportation is persistent. The 2015 bombing of a railway station in Turkey, the 2016 metro bombing in Belgium, and the 2017 metro bombing in Russia demonstrate that terrorists continue to see surface transportation modes as soft targets which can yield high numbers of casualties.

The attempted suicide bombing in the Port Authority Bus Terminal in New York City last month, a few blocks from where I was standing at the time it happened, followed a recent vehicle ramming attack in Manhattan that killed 8 people.

As a Representative of New York's 24th District in Syracuse, I recognize the importance of securing commuter buses, transit agencies, freight rail, and all modes of surface transportation. That is why I am so pleased to be working together with my fellow New Yorker, Chairman Donovan, as well as Ranking Members Watson Coleman and Payne, whose New Jersey transportation systems are so closely linked to those of our home State of New York.

This hearing continues the committee's efforts to understand the challenges facing the diverse spectrum of surface transportation modes as well as the bureaucratic hurdles that stymie the development of security technology.

Previously, we heard from transit police and law enforcement personnel, surface transportation operators, and industry stakeholders. Their insights have helped us to identify obstacles that contribute to an impractical development time line. Security regulations, inspections, VIPR teams, and grants are only parts of the conversations we should be having on how to properly secure surface transportation.

These initiatives must be supplemented by the deployment of innovative security technologies to effectively reduce risk. Based on your experiences and your expertise, I want to know what you all envision as an appropriate balance of security initiatives and technology in the surface transportation environment.

More importantly, I want to know how DHS can lead the way to achieve this balance. In recent testimony, TSA Administrator Pekoske said, "Although we have invested significant resources and implemented numerous programs and policies to reduce identified vulnerabilities and minimize potential consequences, in the current climate, vigilance and preparation can only take us so far." Truer words have not been spoken.

While I do believe that vigilance is a critical part of threat mitigation, I also agree with the administrator that TSA must look beyond existing efforts. We need the effective innovation of security technologies to remain proactive against evolving threats.

Today, I would like to discuss how we can expand upon DHS and TSA's efforts to ensure that stakeholders have the tools they need

to properly secure surface transportation modes. Specifically, how could TSA and S&T better coordinate with each other and with surface transportation stakeholders to streamline the development and deployment of critical security technologies in surface transportation systems?

Ms. Proctor, Mr. Pryor, Mr. Roberts, and Mr. Jenkins, thank you all very much for appearing before us today to testify about this timely and important issue. We look forward to hearing your testimony.

I am pleased to recognize the Ranking Member of the Subcommittee on Transportation and Protective Security, the gentlelady from New Jersey, my friend, Mrs. Watson Coleman, for her opening statement.

[The statement of Chairman Katko follows:]

STATEMENT OF CHAIRMAN JOHN KATKO

JANUARY 30, 2018

The Subcommittee on Transportation and Protective Security and the Subcommittee on Emergency Preparedness, Response, and Communications are meeting today to examine the degree to which the Department of Homeland Security leverages its research and development expertise to improve the security architecture of our Nation's surface transportation systems. Specifically, the subcommittees will examine how the Transportation Security Administration and the Science and Technology Directorate collaborate to improve security capabilities and address identified needs.

The free movement of goods and people depends on the security of our transportation networks. A substantial number of Americans utilize surface transportation on a daily basis, including over 10 billion riders annually on 6,800 U.S. mass transit systems.

While TSA is responsible for securing all of America's transportation systems, its approaches to aviation security and surface transportation security are markedly different. Whereas TSA is directly involved in security operations at airports, the agency provides oversight and assistance to surface transportation modes through partnerships with operators, as well as State and local authorities. This collaborative "whole-of-community" approach helps to ensure that resources are applied efficiently and have the highest efficacy in reducing risk to the Nation's transportation systems. We know that DHS provides support through security threat assessments, explosives detection canines, and security grants; however our subcommittees hope to learn more today of how S&T and TSA are helping to drive security technology innovation for the surface sector. This committee understands that this is a complex undertaking, and I hope we can help you with this critically important responsibility.

The current threat environment facing surface transportation is persistent. The 2015 bombing of a railway station in Turkey, the 2016 metro bombing in Belgium, and the 2017 metro bombing in Russia demonstrate that terrorists continue to see surface transportation modes as soft targets which can yield high numbers of casualties. The attempted suicide bombing in the Port Authority Bus Terminal in New York City last month followed a recent vehicle ramming attack in Manhattan that killed 8 people. As the representative of New York's 24th District, I recognize the importance of securing commuter buses, transit agencies, freight rail, and all modes of surface transportation. That is why I am so pleased to be working together with my fellow New Yorker, Chairman Donovan, as well as Ranking Members Watson Coleman and Payne, whose New Jersey transportation systems are so closely linked to those in our home State of New York.

This hearing continues the committee's efforts to understand the challenges facing the diverse spectrum of surface transportation modes, as well as the bureaucratic hurdles that stymie the development of security technology. Previously, we heard from transit police and law enforcement personnel, surface transportation operators, and industry stakeholders. Their insights have helped us identify obstacles that contribute to an impractical development time line.

Security regulations, inspections, VIPR teams, and grants are only parts of the conversations we should be having on how to secure surface transportation. These initiatives must be supplemented by the deployment of innovative security tech-

nologies to effectively reduce risk. Based on your experiences and your expertise, I want to know what you all envision as an appropriate balance of security initiatives and technology in the surface transportation environment. More importantly, I want to know how DHS can lead the way to achieve this balance.

In recent testimony, TSA Administrator Pekoske said, "Although we have invested significant resources and implemented numerous programs and policies to reduce identified vulnerabilities and minimize potential consequences, in the current climate, vigilance and preparation can only take us so far." While I do believe that vigilance is a critical part of threat mitigation, I also agree with the administrator that TSA must look beyond existing efforts. We need the effective innovation of security technologies to remain proactive against evolving threats.

Today, I would like to discuss how we can expand upon DHS and TSA's efforts to ensure that stakeholders have the tools they need to properly secure surface transportation modes. Specifically, how can TSA and S&T better coordinate with each other and with surface transportation stakeholders to streamline the development and deployment of critical security technologies in surface transportation systems?

Ms. Proctor, Mr. Pryor, Mr. Roberts, and Mr. Jenkins, thank you for appearing before us today to testify about this timely and important issue. We look forward to hearing your testimony.

Mr. KATKO. I am pleased to recognize the Ranking Member of the Subcommittee on Transportation and Protective Security, the gentlelady from New Jersey, my friend, Mrs. Watson Coleman, for her opening statement.

Mrs. WATSON COLEMAN. Thank you, Chairman.

I want to thank you and Chairman Donovan and Ranking Member Payne for convening today's hearing.

Thank you to the panel of witnesses for testifying on this very important topic.

Surface transportation systems, which include freight, passenger trains, commuter rail, mass transit, buses, and pipelines, are vital to the economy of the United States. Every day, millions of Americans rely on these transportation systems. An attack against these systems could be devastating, and terrorists have taken note.

In recent years, terrorists have targeted surface transportation systems overseas, including attacks in London and Brussels. Last month, the threat to public transit systems hit home as a would-be suicide attacker detonated a pipe bomb near Times Square within the New York City subway system. Luckily, the bomb failed to detonate fully, and the bomber was the only person seriously injured.

Nevertheless, the attack proved that the United States is not immune to the types of attacks we have witnessed overseas. The ability of lone-wolf extremists with little to no training, financial support, or direction to carry out attacks against soft targets demands increased attention and collaboration at all levels of government.

Securing such complex, busy transportation systems requires a variety of security measures, including the development and employment of innovative technologies capable of detecting threats without creating congestion.

To develop these new technologies, TSA has established test beds with many of the country's largest mass transit and passenger rail agencies to test promising technologies in the field. While these projects may prove useful, it is clear they do not receive the same attention the aviation technology developments receive.

TSA's recent Biennial Strategic 5-Year Technology Investment Plan Refresh—further referred to by me as Refresh—which lays

out TSA's plans for investing in security technology makes no mention of these projects or of surface transportation at all.

In addition, unlike in aviation, when these technology pilots deliver effective solutions, TSA does not purchase the equipment for deployment. Instead, it falls to local transportation authorities to pay for these technologies, and many of them cannot afford to do so without Federal support.

The American Public Transit Association has testified that transit agencies across the United States have identified $6 billion in capital and operational security requirements. We are currently awaiting the President's fiscal year 2019 budget request, but I would note that, in the face of this massive need and the frightening threat picture, the President's proposed budget for fiscal year 2018 suggests cutting that little Federal support that exists for surface transportation security. The President wants to cut the Transit Security Grant Program, the primary source of Federal security funds for most transit agencies, from $88 million to just $48 million. He wants to cut the TSA's Visible Intermodal Prevention and Response Programs, VIPR, which deploys TSA personnel to conduct security operations at transportation venues from 31 teams to just 8.

These cuts are reckless. We cannot allow this administration to turn a blind eye to the threats facing our surface transportation systems.

That is why I have introduced the Surface Transportation and Public Area Security Act of 2017, which would restore and resource those important activities as well as provide a comprehensive approach to boosting Federal programs aimed at securing these vital systems. Crucially, my bill would authorize $400 million for the Transit Security Grant Program, which would provide a small but significant step in addressing the $16 billion gap in security needs.

That funding would allow transit agencies to purchase some of the innovative technologies our witnesses will discuss today. Additionally, my bill would direct TSA's Innovation Task Force to expand its work beyond aviation security and seek technologies with potential to enhance surface transportation security, providing another avenue for testing new technologies.

My bill would also direct DHS to report to Congress on emerging security technologies within the surface transportation mode, a necessity since such technologies were left out of TSA's recent report. It is time that we finally give surface transportation security the attention it requires, and I look forward to hearing from our witnesses about the challenges they face and how we can be helpful.

Again, I thank my Chairman for convening this hearing, and I yield back the balance of my time.

[The statement of Mrs. Watson Coleman follows:]

STATEMENT OF RANKING MEMBER BONNIE WATSON COLEMAN

JANUARY 30, 2018

Surface transportation systems, which include freight and passenger trains, commuter rail, mass transit, buses, and pipelines, are vital to the economy of the United States. Every day, millions of Americans rely on these transportation systems. An attack against these systems could be devastating—and terrorists have taken note.

In recent years, terrorists have targeted surface transportation systems overseas, including attacks in London and Brussels. Last month, the threat to public transit

systems hit home, as a would-be suicide attacker detonated a pipe bomb near Times Square, within the New York City subway system. Luckily, the bomb failed to detonate fully, and the bomber was the only person seriously injured.

Nevertheless, the attack proved that the United States is not immune to the types of attacks we have witnessed overseas. The ability of "lone-wolf" extremists with little to no training, financial support, or direction to carry out attacks against soft targets demands increased attention and collaboration at all levels of government.

Securing such complex, busy transportation systems requires a variety of security measures, including the development and deployment of innovative technologies capable of detecting threats without creating congestion.

To develop new technologies, TSA has established "test beds" with many of the country's largest mass transit and passenger rail agencies to test promising technologies in the field.

While these projects may prove useful, it is clear they do not receive the same attention that aviation technology development receives. TSA's recent "Biennial Strategic Five-Year Technology Investment Plan Refresh," which lays out TSA's plans for investing in security technology, makes no mention of these project—or of surface transportation at all.

In addition, unlike in aviation, when these technology pilots deliver effective solutions, TSA does not purchase the equipment for deployment. Instead, it falls to local transportation authorities to pay for these technologies, and many of them cannot afford to do so without Federal support. The American Public Transit Association has testified that transit agencies across the United States have identified $6 billion in capital and operational security requirements.

We are currently awaiting the President's fiscal year 2019 budget request, but I would note that, in the face of this massive need and a frightening threat picture, the President's proposed budget for fiscal year 2018 suggests cutting what little Federal support exists for surface transportation security.

The President wants to cut the Transit Security Grant Program—the primary source of Federal security funds for most transit agencies—from $88 million to just $48 million. He wants to cut TSA's Visible Intermodal Prevention and Response (VIPR) program—which deploys TSA personnel to conduct security operations at transportation venues—from 31 teams to just 8. These cuts are reckless. We cannot allow this administration to turn a blind eye to the threats facing our surface transportation systems.

That is why I have introduced the Surface Transportation and Public Area Security Act of 2017, which would restore and resource these important activities, as well as provide a comprehensive approach to boosting Federal programs aimed at securing these vital systems.

Crucially, my bill would authorize $400 million for the Transit Security Grant Program, which would provide a small but significant step in addressing the $6 billion gap in security needs. That funding would allow transit agencies to purchase some of the innovative technologies our witnesses will discuss today.

Additionally, my bill would direct TSA's Innovation Task Force to expand its work beyond aviation security and seek technologies with potential to enhance surface transportation security, providing another avenue for testing new technologies. My bill would also direct DHS to report to Congress on emerging security technologies within the surface transportation mode—a necessity since such technologies were left out of TSA's recent report.

It is time that we finally give surface transportation security the attention it requires.

Mr. KATKO. Thank you, Mrs. Watson Coleman.

I now recognize the Chairman of the Subcommittee on Emergency Preparedness, Response, and Communications, my friend Mr. Donovan, for an opening statement.

Mr. DONOVAN. Thank you, Mr. Chairman, and thank you for convening our subcommittees together for this very important hearing.

Surface transportation systems serve over 10 billion riders annually. Like me—because I am one of those riders; I take Amtrak back and forth from New York City to Washington every week—these people depend on the reliability and safety of this critical infrastructure and so does our economy. The open systems, multiple hubs, and lack of screening has made surface transportation sys-

tems a target for terrorist organizations and their sympathizers for years.

We have seen attacks in Brussels, London, and, most recently, in New York City. Last December, one such terrorist tried to detonate a suicide bomb in a walkway underneath the Port Authority Bus Terminal during rush hour. Thankfully, he constructed a faulty IED. However, this attempted terrorist attack is a stark reminder of how vulnerable our surface transportation systems are to terrorist attacks.

Surface transportation system operators are continuously looking for innovative technology to help create a multi-layer approach to security. However, this search for technology solutions has been bogged down by numerous obstacles. That is why both of our subcommittees have been extensively looking at how technology can help make our surface transportation systems more secure without impeding their operations.

Last November, our subcommittees held a roundtable with surface transportation system operators and heard some of the challenges that they face when trying to integrate new technology into their systems. Specifically, technology that is deemed to be successful in a lab doesn't always work once it is integrated into a mass transit system. Thus, there needs to be a test bed and pilot locations to adequately test new technology. There is a need for a technology clearinghouse where operators can review impartial assessments of the technology that is available to them.

Now it is time for us to hear from the Department of Homeland Security, specifically TSA and S&T, on how they are helping surface transportation operators with research and development, test and evaluation, and other issues surrounding new technology. I am interested in learning more about how S&T and TSA are working together to ensure our surface transportation operators have the tools and resources they need to keep the riders safe, specifically with regard to technology.

I want to also thank our witnesses for their time, their expertise, and what they are doing for our riders on a daily basis, and for this afternoon for being here to share your expertise with us. I look forward to our discussion.

With that, Mr. Chairman, I yield back.

[The statement of Chairman Donovan follows:]

STATEMENT OF CHAIRMAN DANIEL M. DONOVAN, JR.

JANUARY 30, 2018

Surface transportation systems serve over 10 billion riders annually. Like me—I am one of those 10 billion riders—these people depend on the reliability and safety of this critical infrastructure, and so does our economy.

The open systems, multiple hubs, and lack of screening has made surface transportation systems a target for terrorist organizations and their sympathizers for years. We have seen attacks in Brussels, London, and most recently in New York City.

Last December, Akayed Ullah tried to detonate a suicide bomb in a walkway underneath the Port Authority Bus Terminal during rush hour. Thankfully, he constructed a faulty IED. However, this attempted terrorist attack is a stark reminder of how vulnerable our surface transportation systems are to terrorist attacks.

Surface transportation system operators are continuously looking for innovative technology to help create a multi-layer approach to security. However, this search for technological solutions has been bogged down by numerous obstacles.

That is why both of our subcommittees have been extensively looking at how technology can help make our surface transportation systems more secure, without impeding their operations.

Last November, our subcommittees held a roundtable with surface transportation system operators and heard some of the challenges they face when trying to integrate new technology into their systems. Specifically,

- Technology that is deemed successful in a lab doesn't always work once integrated into a mass transit system. Thus, there is a need for test beds and pilot locations to adequately test this technology. And,
- There is a need for a technology clearinghouse where operators can review impartial assessments of the technology available to them.

Now, it is time for us to hear from the Department of Homeland Security, specifically TSA and S&T, on how they are helping surface transportation operators with research and development, test and evaluation, and other issues surrounding new technology. I'm interested in learning more about how S&T and TSA are working together to ensure our surface transportation operators have the tools and resources they need to keep the riders safe, specifically with regard to technology.

I want to thank the witnesses for being here this afternoon and I look forward to our discussion.

Mr. KATKO. Thank you, Mr. Donovan. I am very pleased that our two subcommittees are working together to address this very important issue.

Before I introduce the next chair of the subcommittee, I want to just caution all the witnesses here, the way the votes are lining up, we may have to truncate this hearing a little bit. So, for the next few minutes, perhaps you can think in your mind how to shorten your opening statements as best you can so we can have more times for questions.

With that, I will now recognize the Ranking Member of the Subcommittee on Emergency Preparedness, Response, and Communications, Mr. Payne, for an opening statement.

Mr. PAYNE. Thank you, and good afternoon. I would like to thank Chairman Katko and Donovan, as well as Ranking Member Watson Coleman, for holding today's hearing to assess the Department of Homeland Security's efforts to develop and identify novel surface transportation security technologies.

I represent Newark and Jersey City, which are two of the largest cities in the State of New Jersey. Every day, my constituents rely on New Jersey Transit, the PATH train, and Amtrak trains to commute within the tri-State area.

Two years ago, following a horrific attack on the Brussels metro system, I was pleased that my subcommittee held a field hearing in my district to learn more about how the Federal Government could help prevent a similar incident from happening in the busiest surface transportation corridors in the country. At the hearing, we also considered how first responders coordinate with transit owners and operators to ensure we are prepared if, God forbid, such an attack did occur.

We brought together representatives from the Transportation Security Administration, the Port Authority of New York and New Jersey, New Jersey Transit, New York City's Metropolitan Transportation Authority, and Amtrak and had a robust discussion. There were two major takeaways.

The vast majority of TSA's resources support securing aviation travel. So the preliminary responsibility for securing surface transportation infrastructure falls on owners and operators. Owners and operators rely on the DHS Transit Security Grant Program funding

to install and maintain technology and security operations to keep transit systems secure without jeopardizing passenger flow.

These findings were reiterated at the field hearing held in Mrs. Watson Coleman's district late last year. As Ranking Member of the Emergency Preparedness Subcommittee, I have fought for the TSGP funding and to ensure that the Department's research and development efforts are responsive to the threat environment and needs of transit owners and operators.

So, when the President released his fiscal year 2018 budget last year, I was troubled to see that he proposed slashing TSGP grants funding by 52 percent. On top of that, the President's budget proposed to gut the Urban Area Security Initiatives and the State Homeland Security Grant Program by over $270 million. DHS's suite of grant programs work in concert to make high-risk targets, like our surface transit systems, more secure. Attempts to cut them in this threat environment reflect a genuine disconnect from reality.

As we anticipate the fiscal year 2019 budget proposal, I hope the administration has come to its senses and will request more adequate funding for these important programs. Moreover, I hope that Congress enacts a full year spending bill for fiscal year 2018 so the grant funds are made available to our communities to make surface transportation more secure.

Before I close, I would like to acknowledge that the President's fiscal year 2018 budget also made dramatic cuts to the Science and Technology Directorate. Although much of S&T transportation work was not affected, other programs that could complement its surface transportation efforts were. I implore the administration to submit a responsible budget that recognizes the connectivity between various important S&T research programs.

In the mean time, I will continue to support H.R. 4474, Mrs. Watson Coleman's Surface Transportation and Public Area Security Act, which addresses pressing transportation security gaps, and I urge my colleagues to do the same.

With that, Mr. Chairman, I yield back.

[The statement of Ranking Member Payne follows:]

STATEMENT OF RANKING MEMBER DONALD M. PAYNE, JR.

JANUARY 30, 2018

I represent Newark and Jersey City, which are two of the largest cities in the State of New Jersey. Every day, my constituents rely on New Jersey Transit, PATH, and Amtrak trains to commute within the tri-State area.

Two years ago, following a horrific attack on the Brussels metro system, I was pleased that my subcommittee held a field hearing in my district to learn more about how the Federal Government could help prevent a similar incident from happening in the busiest surface transportation corridors in the country. At the hearing, we also considered how first responders coordinate with transit owners and operators to ensure we are prepared if—God forbid—such an attack did occur. We brought together representatives from the Transportation Security Administration, the Port Authority of New York and New Jersey, New Jersey Transit, New York City's Metropolitan Transportation Authority, and Amtrak, and had a robust discussion.

There were two major takeaways. The vast majority of TSA's resources support securing aviation travel, so the primary responsibility for securing surface transportation infrastructure falls on owners and operators. Owners and operators rely on the DHS Transit Security Grant Program (TSGP) funding to install and maintain technology and security operations that keep transit systems secure without jeop-

ardizing passenger flow. These findings were reiterated at the field hearing held in Ms. Watson Coleman's district late last year.

As Ranking Member of the Emergency Preparedness Subcommittee, I have fought for TSGP funding and to ensure that the Department's research and development efforts are responsive to the threat environment and needs of transit owners and operators.

So when the President released his fiscal year 2018 budget last year, I was troubled to see that he proposed slashing TSGP grant funding by 52 percent. On top of that, the President's budget proposed to gut the Urban Area Security Initiative and the State Homeland Security Grant Program by over $270 million.

DHS's suite of grant programs work in concert to make high-risk targets—like our surface transit systems—more secure. Attempts to cut them in this threat environment reflect a genuine disconnect from reality. As we anticipate the fiscal year 2018 budget proposal, I hope the administration has come to its senses and will request more adequate funding for these important programs.

Moreover, I hope that Congress enacts a full year spending bill for fiscal year 2019 so that grant funds are made available to our communities to make surface transportation more secure.

Before I close, I would like to acknowledge that the President's fiscal year 2018 budget also made dramatic cuts to the Science and Technology Directorate. Although much of S&T's transportation work was not affected, other programs that could complement its surface transportation efforts were. I implore the administration to submit a responsible budget that recognizes the connectivity between various important S&T research programs.

In the mean time, I will continue to support H.R. 4474, Ms. Watson Coleman's Surface Transportation and Public Area Security Act, which addresses pressing transit security gaps, and I urge my colleagues to do the same.

Mr. KATKO. Thank you, Mr. Payne.

Other Members of the subcommittee 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

JANUARY 30, 2018

When it comes to transportation security, aviation security dominates the conversation throughout the Government, but given the diversity of today's terrorist landscape, it is well past time for the conversation to expand.

We all well know that in recent years, surface transportation systems both overseas and at home have increasingly been a target of lethal mass casualty attacks.

Last October, a terrorist in Manhattan ran a vehicle onto a bike bath killing 8 people and injuring 11.

Just last month, a terrorist strapped a home-made explosive device onto his body and detonated it in the New York City's subway. While the blast was not powerful enough to kill, 4 innocent commuters sustained injuries.

These recent cases indicate that, in the age of lone-wolf and small-cell attacks, the targeting of mass transit and other surface transportation centers is growing.

Further, surface transportation systems in Madrid, London, Paris, and Brussels have all been targeted by terrorists.

Therefore, there is no sensible justification for surface transportation security to garner only 2 percent of the Transportation Security Administration's budget.

Additionally, it is incumbent upon Congress to re-examine TSA's budget allocations for surface transportation security. It is our job to make sure that DHS is positioned to address this emerging terrorist threat.

I want to thank Ranking Member Watson Coleman for her leadership on surface transportation security. Her legislation, the Surface Transportation and Public Area Security Act of 2017, would restore, revamp, and resource important programs vital to protecting our Nation's surface transportation systems.

I hope today's conversation will focus on how DHS can do more to partner with stakeholders to make these systems more secure and resilient.

As we have seen with aviation sector, the introduction of innovative technological solutions is essential to strengthening the security of surface transportation.

To our witnesses, if there is technology on the cusp of development that needs research and development funding from Congress, let us know, we want to be helpful. If there are authorities that DHS needs to address surface transportation threats, tell us.

To my colleagues, I know we are expecting to see the fiscal year 2019 budget proposal from the Trump administration in the coming weeks.

If you recall, the President Trump's fiscal year 2018 budget proposed cutting $43 million in surface transportation security. In the event that the forthcoming budget proposes similar cuts to surface transportation, I hope you will join me in opposing such cuts.

As evidenced by the testimony and participation in today's hearing, now is not the time to make drastic, unjustified, and illogical cuts to our security. I look forward to engaging with both the witnesses and my colleagues on surface transportation security, not only here today, but also in the future.

Mr. KATKO. We are grateful to have before us this afternoon a distinguished panel here to testify. Let me remind each of the witnesses, as I have alluded to, that we are under a time crunch, No. 1; and, No. 2, their entire written statement will appear in the record.

Our first witness, Ms. Sonya Proctor, serves as a deputy of the surface division—I am sorry—the director of the Surface Division within the Transportation Security Administration's Office of Security Policy and Industry Engagement. In this role, she is responsible for developing risk-based security policy in conjunction with stakeholders for surface transportation modes.

Prior to this position, Ms. Proctor served as a deputy federal secretary—security director at Ronald Reagan National Airport in Washington, DC. Ms. Proctor has a long tenure of law enforcement service, beginning with the Washington, DC, Metropolitan Police Department. Ms. Proctor went on to serve as a chief of police for the National Amtrak Police Department, developing a new strategic plan to city policing and a passenger railroad environment.

Ms. Proctor, thank you very much for your service and for your continuing service to our country and in your current role. I now recognize Ms. Proctor for her opening statement.

STATEMENT OF SONYA PROCTOR, DIRECTOR, SURFACE DIVISION, OFFICE OF SECURITY POLICY AND INDUSTRY ENGAGEMENT, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. PROCTOR. Thank you. Good afternoon, Chairman Katko, Chairman Donovan, Ranking Member Watson Coleman, Ranking Member Payne, and distinguished Members of the subcommittees. Thank you for the opportunity to testify today about TSA's role in surface transportation security technology.

TSA appreciates the continued support of this committee and its Members as we carry out our vital security mission. We are grateful for the constructive relationship TSA enjoys with this committee and look forward to our continued work together to ensure the security of our Nation's transportation systems.

As the director for the Surface Division within TSA's Office of Security Policy and Industry Engagement, I have the responsibility for overseeing the development of risk-based surface transportation security policies in collaboration with industry operators and other Federal agencies to develop and implement those policies.

To illustrate the magnitude and importance of the surface transportation system, which is moving people and commodities on a continuous basis, consider that over 11 million passengers daily travel on New York MTA system alone. Every year, more than 10 billion trips are taken on 6,800 U.S. mass transit systems, which

range from very small bus-only systems in rural areas to very large multimodal systems like the New York MTA in major cities. Almost 4,000 commercial bus companies travel on the 4 million miles of roadway in the United States and on more than 600,000 highway bridges and through 350 tunnels. Those same roads, bridges, and tunnels support the movement of goods throughout the country by 8 million large-capacity commercial trucks. As for our railroads and pipelines, more than 500 individual freight railroads carry essential goods operating on nearly 140,000 miles of track, and 2.5 million miles of pipelines owned and operated by approximately 3,000 private companies transport natural gas, refined petroleum products, and other commercial products.

When assessing risk in any particular transportation mode, TSA considers the threat, the vulnerability, and the consequence should an incident occur. TSA takes the threat to surface transportation mode very seriously.

Recent terror attacks and plots, like the attempted suicide bombing in the New York City Port Authority Bus Terminal and the vehicle ramming attack in Manhattan, serve as compelling reminders of the vast challenges of securing a system of systems that is designed to quickly move massive volumes of passengers and commodities.

Unlike aviation, where TSA is heavily involved in executing day-to-day security operations, our approach for surface transportation security is different. It is one focused on supporting, collaborating, and partnering with the owners and operators of the systems. The interconnected varied and expansive scope of the surface transportation system creates unique security challenges that are best addressed by system owners and operators and Federally supported through stakeholder communication, coordination, and collaboration.

To that end, TSA focuses its efforts on system assessments, voluntary operator compliance with industry standards, collaborative law enforcement and security operations, accurate and timely exchange of intelligence information, regulatory oversight, and technology expertise. My colleague, Robert Pryor, who is director for TSA's Intermodal Division within the Office of Requirements and Capabilities Analysis will further explain through his testimony the work TSA does to assist surface owners and operators identify vulnerabilities and risks in their operations and the role TSA plays in that process.

Again, thank you for the opportunity to be here today. I am happy to answer any questions you may have.

[The joint prepared statement of Ms. Proctor and Mr. Pryor follows:]

JOINT PREPARED STATEMENT OF SONYA PROCTOR AND ROBERT PRYOR

JANUARY 30, 2018

Good morning Chairmen Katko and Donovan, Ranking Members Watson Coleman and Payne, and distinguished Members of the subcommittees. We are grateful for the opportunity to appear before you to discuss the Transportation Security Administration's (TSA) efforts regarding surface transportation security and technology initiatives. Today's hearing is timely, as technology deployment for both aviation and surface transportation systems will be critical to TSA's success in 2018 and beyond.

TSA appreciates the continued support of this committee and its Members, as we carry out our vital security mission. We are grateful for the constructive relationship TSA enjoys with this committee, and look forward to our continued work together to ensure the security of our Nation's transportation systems.

The U.S. surface transportation system, which is comprised of roads, bridges, tunnels, mass transit systems, passenger and freight railroads, over-the-road bus operators, motor carrier operators, pipelines, and maritime facilities, is an extremely complex, interconnected, and largely open network. The various transportation modes within this system operate daily in close coordination with and proximity to one another. In fact, many of the modes use the same roads, bridges, and tunnels to function. Americans and our economy need and depend on the surface transportation system to operate securely and safely.

To illustrate the magnitude and importance of the system, which is moving people and commodities on an essentially continuous basis, consider that over 11 million passengers daily travel on the New York Metropolitan Transportation Authority (NY MTA) system alone. Every year more than 10 billion trips are taken on 6,800 U.S. mass transit systems, which range from very small bus-only systems in rural areas to very large multi-modal systems, like the NY MTA, in major cities. Over-the-road bus operators carry approximately 750 million intercity bus passengers each year. Almost 4,000 commercial bus companies travel on the 4 million miles of roadway in the United States and on more than 600,000 highway bridges greater than 20 feet in length and through 350 tunnels greater than 300 feet in length. Those same roads, bridges, and tunnels support the movement of goods throughout the country by 8 million large capacity commercial trucks. As for our railroads and pipelines, more than 500 individual freight railroads carrying essential goods operate on nearly 140,000 miles of track, and 2.5 million miles of pipelines, owned and operated by approximately 3,000 private companies, transport natural gas, refined petroleum products, and other commercial products.

As these facts demonstrate, securing surface transportation is both a critically important and complex undertaking. Recent terror attacks and plots—like the attempted suicide bombing in the New York City Port Authority Bus Terminal and vehicle ramming attack in Manhattan, serve as compelling reminders of the vast challenges of securing a "system of systems" that is designed to quickly move massive volumes of passengers and commodities.

When assessing risk in any particular transportation mode, TSA considers the threat, the vulnerability, and the consequence, should an incident occur. TSA takes the threat to the surface mode very seriously. Although we have invested significant resources and implemented numerous programs and policies to reduce identified vulnerabilities and minimize potential consequences, in the current climate, vigilance and preparation can only take us so far. For this reason, TSA is reexamining its approaches and actively assessing how best to leverage and enhance its surface expertise to strengthen our partnership with surface stakeholders.

Unlike aviation, where TSA has been heavily involved in day-to-day security operations since the agency was created in 2001, we have primarily approached surface transportation security as a partnership with the owners and operators of the system. This difference in approach is reflective of the characteristics of the system. The interconnected, varied, and expansive scope of the surface transportation system creates unique security challenges that are best addressed by system owners and operators and Federally supported through stakeholder communication, coordination, and collaboration. To best assist surface transportation owners and operators with their security needs, TSA focuses its efforts on system assessments, voluntary operator compliance with industry standards, collaborative law enforcement and security operations, accurate and timely exchange of intelligence information, regulatory oversight, and technology expertise.

TSA invests its resources to help surface owner and operators identify vulnerabilities and risks in their operations, and then works with them to develop and implement risk-mitigating solutions to address them. The inherently open and expansive scope of surface passenger transportation and the evolving threat to it requires TSA to continue researching and developing innovative processes and technologies to increase security without creating undesired financial or operational burdens. Engagement and partnership with surface transportation owners and operators is the key to fostering innovation and ensuring the system is secure both today and in the future.

TSA incorporates the needs and capability gaps of surface transportation owners and operators into our work to influence and stimulate the development of new security technologies in the marketplace. Our approach is designed to make more readily available innovative and advanced technologies useful for public area security. TSA actively follows the fast-moving advancement of security technologies to

assess whether emerging technologies, including from outside the transportation environment, could be applied to address current and evolving threats to the surface transportation system.

TSA accomplishes this goal through its Intermodal Division by working closely with surface transportation owners and operators to introduce new technology and approaches to securing surface transportation. We establish collaborative operational test beds for different modes of transportation (mass transit, highway motor carrier, pipeline, and freight rail), and critical infrastructure protection security technology projects to address the increasing threat demonstrated from attacks world-wide. TSA's Intermodal Division's Surface program was established in 2004 following the Madrid and London attacks and has been fostering "innovation" within the surface transportation system for more than a dozen years. Working in conjunction with the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T), TSA's Intermodal Division provides security technology recommendations and solutions for surface and aviation transportation venues by evaluating existing security technologies and developing requirements for new technologies. The Division's mission areas reflect provisions in the Implementing Recommendations of the 9/11 Commission Act of 2007 and other public laws, Executive Orders, and National policies and plans.

Since its creation, the Intermodal Division has stimulated the marketplace and assessed numerous technologies, ranging from those effective and suitable for person-borne threats to technology that protects critical infrastructure, to detection of chemical and biological threats. TSA is also a National leader in providing analysis tools and mitigation means for explosive blast in passenger rail vehicles.

TSA's surface security technology program has progressed as threats and risk have grown, with the expectation that threats overseas would eventually manifest in the United States. Our efforts have included short-term technology demonstrations in venues such as the Port Authority of New York and New Jersey's PATH system and the Manhattan Bus Terminal, Amtrak, Staten Island Ferry terminals, NY Mass Transit Authority infrastructure, ferry terminals in Long Island and Cape May, hazardous materials pipeline cybersecurity vulnerability assessments and mitigation recommendations, and infrastructure protection work in the Newark and Jersey City areas.

TSA has formal agreements with leading and higher-risk surface venues to serve as test beds for promising technology. New Jersey Transit Police was TSA's first test bed partner over 10 years ago and continues to work with us on assessing various technologies to address their security needs. In fact, TSA currently has on-going test beds with 5 of the 10 highest-risk mass transit and passenger rail venues, and agreements in principle from NY MTA and Port Authority for the World Trade Center Oculus. We also have agreements in principle with Los Angeles World Airports Authority and Burbank Airport to serve as public area security testbed partners. The results of that public area security technology testing will support potential use in both surface and aviation venues. Finally, TSA has formal agreements with several freight railroads for technology to protect key rail infrastructure such as bridges, high-risk rail lines in urban areas, and rail yards, as well as with the Nation's largest hazardous materials pipeline operator.

For example, TSA is presently working with New Jersey Transit, Washington Metropolitan Transit Authority, Amtrak, and Los Angeles Metro to assess the effectiveness of technologies designed to address threats associated with person- and vehicle-borne improvised explosive devices. Through such efforts, as well as intelligence, information sharing, and active engagement with surface owners and operators, TSA helps technology manufacturers develop their products to better meet the security needs of the surface transportation system, and serves as the technology surrogate for the many smaller transportation authorities that cannot afford or support expensive technology development and assessments. As a result of TSA's security technology support efforts, surface owners and operators can make informed decisions about funding and acquiring security technologies to meet their operational needs.

TSA and DHS S&T are long-term and close collaborators. We have a clear understanding of each other's roles and missions and take great care to optimize our work together. DHS S&T specializes in longer-term research and development (R&D) and proof of concept technologies while TSA engages the marketplace for technologies that are more mature. In most cases, TSA is considering pre-production prototypes that can immediately benefit from operational user feedback and stimulus to enter the marketplace more rapidly. As needed, TSA makes its test beds available to DHS S&T for early user impressions of emergent R&D technology and design recommendations.

TSA is committed to securing the Nation's surface transportation system from terrorist activities and attacks. Chairmen Katko and Donovan, Ranking Members Watson Coleman and Payne, and distinguished Members of the subcommittees, thank you for the opportunity to testify before you today. We are honored to serve in this capacity and look forward to your questions.

Mr. KATKO. Thank you, Ms. Proctor.

Our second witness, Mr. Robert Pryor, is assigned to the Office of Operational Requirements and Capabilities Analysis at the TSA as a director of the Intermodal Division.

The Intermodal Division supports requirements, development, and field and laboratory assessments of security technologies for all TSA mission areas, except civil aviation passenger screening. Mr. Pryor is a former Marine officer, and has Active Duty experience, including a variety of fleet maritime force command and specialized counterterrorism assignments.

Sir, thank you for your service to our country and your dedication to our country as well. The Chair now recognizes the Mr. Pryor for his opening statement.

STATEMENT OF ROBERT PRYOR, DIRECTOR, INTERMODAL DIVISION, OFFICE OF REQUIREMENTS AND CAPABILITIES ANALYSIS, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. PRYOR. Good afternoon, Chairman Katko and Chairman Donovan, Ranking Member Watson Coleman, Ranking Member Payne, and distinguished Members of the Committee of Homeland Security.

Mr. Katko, congratulations on your son's graduation. That is a notable achievement. I have spent a little time in Fort Benning, and it is not easy.

Mr. KATKO. It is quite an adventure for him, I got to tell you. He is going to go to ranger school in June as well, so that will be even more of an adventure.

Mr. PRYOR. Yes, sir, absolutely. Thank you for the opportunity to appear before you to discuss surface transportation technology initiatives that TSA is working on to assist surface transportation owners and operators protecting our transportation system.

Since its creation in 2004, following the Madrid and London attacks, the Intermodal Division has stimulated the marketplace and assessed numerous technologies, ranging from those effective and suitable for person-borne threats to technology that protects critical infrastructure to detection of chemical and biological threats. TSA is also a national leader in providing analysis tools and mitigation means for explosive blast and passenger rail vehicles.

TSA continuously researches and develops innovative processes and technologies to increase security without creating undesired financial or operational burdens. We are all aware that mass transit, in particular, riders are particularly sensitive to fare increases, and we keep that in mind.

First, TSA helps surface owners and operators identify vulnerabilities and risks in their operations and then works with them to develop and implement risk-mitigating solutions to address the vulnerabilities.

Next, TSA incorporates the needs and capability gaps of surface transportation owners and operators into our work to influence and

stimulate the development of new security technologies in the marketplace.

TSA actively follows the advancement of security technologies to assess whether emerging technologies, including from outside the transportation environment, could be applied to address current and evolving threats.

Third, and to that end, TSA's Intermodal Division works closely with transportation stakeholders to introduce new technologies and approaches to securing transportation. We establish collaborative operational test beds for different modes of transportation and critical infrastructure protection security technologies to address the incoming threat demonstrated from attacks world-wide.

TSA currently has on-going test beds with 5 of the 10 highest-risk mass transit and passenger rail venues and is now also working with additional public area security partners.

TSA also has formal agreements with several freight railroads for technology to protect key rail infrastructure, such as bridges, high-risk rail lines in urban areas and rail yards, as well as with the Nation's largest hazardous material pipeline operator.

TSA shares the results of its testing with all of the stakeholders and also technology manufacturers to assist them in improving their products. We also serve as the technology surrogate for many smaller transportation authorities that cannot afford or support expensive technology development assessment.

As a result of TSA's security technology support efforts, owners and operators can make more informed decisions about funding and acquiring security technologies to meet their operational needs.

Thank you very much for the opportunity to testify before you today. I am honored to be here and look forward to your questions.

Mr. KATKO. Thank you, Mr. Pryor.

Our third witness, Mr. Donald Roberts, serves as a program manager for the Surface Transportation Explosive Threat Detection Program for the Explosives Division within the Homeland Security Advanced Research Projects Agency, Science and Technology Directorate.

Mr. Roberts has been with the DHS since 2006. He came there with over 18 years of experience with the Department of Defense, where he managed advanced research development test and evaluation programs. The Chair now recognizes Mr. Roberts for his opening statement.

STATEMENT OF DONALD E. ROBERTS, PROGRAM MANAGER, EXPLOSIVE THREAT DETECTION, EXPLOSIVES DIVISION, HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY, SCIENCE AND TECHNOLOGY DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. ROBERTS. Thank you. Chairmen Katko and Donovan, Ranking Members Payne, Watson Coleman, and distinguished Members of the subcommittees, thank you for the opportunity to discuss Department of Homeland Security Science and Technology Directorate's work in assisting surface transportation agencies, as well as how S&T works collaboratively with the Transportation Security Administration in this area.

S&T, Science and Technology, Explosives Division enjoys a close working relationship with TSA's Intermodal Division, the Office of Security Policy and Industry Engagement, and with public and private-sector partners to address security gaps in the Nation's transportation network.

The unique challenges of this open system with no fixed checkpoints, extremely high passenger throughput, the need to maintain traveler privacy, and physical safety of both the traveling public and system operators, as well as an unalterable existing infrastructure within which technologies for threat detection must fit necessitates a dedicated program focused specifically on this significant capability gap.

The S&T Surface Transportation Program goal is to develop a layered detection system consisting of a suite of sensors capable of identifying person-borne threat items with a high probability of detection and a low probability of false alarm, providing a curb-to-platform layered threat detection system.

We are also advancing the state-of-the-art of intelligent video and video analytics tools to improve detection of leave-behind bags and quickly highlighting the surrounding circumstances of how the bag was left to provide actionable situational awareness of a potential threat. These tools are currently in use at the Washington Metropolitan Area Transit Authority Security Operation Center here in the District of Columbia, and we are planning to transition the capability to a broader Nation-wide end-user community through a commercial partnership by 2019.

In addition to electronic technology solutions, DHS Science and Technology Detection Canine Program has also undertaken an effort to focus on the person-borne improvised explosive, or PBIED, detection canine. Canines are the most versatile mobile detections tools we have to protect the homeland today, and S&T's PBIED canine initiative was created to assess strengths and limits of canines specially trained to detect threats being carried by people either on their persons or in bags in mass transit and large crowd event venues.

This type of parametric study and testing had not previously been undertaken in the global detection canine community. S&T has taken the lead to conduct this type of parametric study, which is critical to understanding the limits of performance for the canine detection teams in these types of search applications.

Chairman Donovan, Katko, Ranking Members Payne and Watson Coleman, distinguished Members of the committee, thank you again for your attention to this important mission and for the opportunity to discuss S&T support to TSA and the surface transportation agencies.

[The prepared statement of Mr. Roberts follows:]

PREPARED STATEMENT OF DONALD E. ROBERTS

JANUARY 30, 2018

Chairman Donovan, Chairman Katko, Ranking Member Payne, Ranking Member Watson Coleman, and distinguished Members of the committees, thank you for inviting DHS to speak with you today. I appreciate the opportunity to discuss the Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) work in assisting surface transportation agencies, as well as how S&T works col-

laboratively with the Transportation Security Administration (TSA) in this mission area.

I have been the Surface Transportation Explosive Threat Detection (STETD) program manager since the program's inception in fiscal year 2011, and have been with the Department since 2006. Prior to my time at DHS, I was a research, development, test, and evaluation program manager for special programs within DoD focusing on Army aviation and missile systems, and have worked to develop technology addressing critical operational gaps from idea to fielding throughout my entire career.

S&T's Explosive Division enjoys a close working relationship with TSA's Intermodal Division to ensure the security of our Nation's transportation systems. The Implementing Recommendations Section 1409 of the 9/11 Commission Act of 2007, Pub. L. 110–53, (codified at 6 U.S.C. 1138) requires the DHS Secretary to carry out an R&D program through the S&T Homeland Security Advanced Research Projects Agency (HSARPA) and in consultation with Transportation Security Administration (TSA) for the purpose of improving the security of public transportation systems. S&T appreciates the continued support of this committee and its Members, as we carry this vital security mission, and are grateful for the opportunity to foster a stronger constructive relationship in the future

The U.S. surface transportation network is immense, consisting of buses, passenger and freight railroads, and ferries. DHS has been working diligently with public and private-sector partners to address security gaps in the Nation's transportation network. The challenge is how to address a decentralized, diffuse, complex, and evolving terrorist threat in the context of an inherently open and diverse surface transportation system. The two competing challenges of this need are the ability to provide credible, real-time detection capabilities without interrupting the rapid movement of passengers.

Public safety officials have little to no capability to detect threats being carried into surface transportation venues. They must rely on intelligence reports before an attack or public reporting of events already under way. There is often no awareness until after an attack has already occurred.

DHS S&T has a number of programs/pilots under way to address the identified security needs in the surface transportation sector. The DHS S&T Surface Transportation Explosive Threat Detection (STETD) program was designed to develop a layered detection system consisting of a suite of sensors capable of identifying person-borne threat items, with a high probability of detection and low probability of false alarm. The DHS S&T role is to develop such technology through Developmental Test and Evaluation (DT&E) and then work with TSA's Office of Requirements and Capabilities Analysis (ORCA) Intermodal Division to move into Operational Test and Evaluation (OT&E), and ultimately transition to a commercial partner.

The STETD program began in fiscal year 2011 working with the TSA by defining site-specific requirements through surface transportation venue assessments, and identifying capability gaps captured via Homeland Security Enterprise organizations. After visiting several surface transit venues of varying sizes (large, medium, and small), meeting with owners/operators and security personnel, surveying commercial technologies, and reviewing technology development efforts across Government agencies and the National laboratories, it was determined there was no existing solution meeting the requirements posed by this very challenging environment.

The unique challenges of an open system with no fixed checkpoints, extremely high passenger throughput, the need to maintain traveler privacy, and the physical safety of both the traveling public and system operators, and an unalterable existing infrastructure within which technologies for threat detection must fit, necessitates a dedicated program focused specifically on this significant capability gap. Therefore, DHS created a technology development pathway specific to the challenge.

The program is developing prototype stand-off detection sensors, with the vision of providing "curb to platform" layered threat detection distributed throughout a surface transportation venue. The STETD program is also advancing research and development of Intelligent Video/Video Analytics (IV/VA) algorithms to improve detection of leave-behind bags and quickly highlight the surrounding circumstances of how the bag was left to provide actionable situational awareness of a potential threat. The Forensic Video Exploitation and Analysis (FOVEA) analytics tool suite, developed within the STETD program, enables the operators to save resources on response call-outs; compress long durations of surveillance video into much shorter clips reducing review effort from days to hours; and helps operators follow individuals of interest across multiple camera views. The system is currently in use at Washington Metropolitan Area Transit Authority (WMATA) Special Operations Center, and S&T is planning to transition the capability to the broader Nation-wide end-user community through a commercial partner by fiscal year 2019.

In addition to technology solutions, DHS S&T's Detection canine program has also undertaken an effort to focus on the Person-Borne Improvised Explosive Device (PBIED) detection canine. Canines are the most versatile mobile detection tools that we have to protect the homeland today, and S&T's PBIED canine initiative was created to assess the strengths and limits of canines specially trained to detect threats being carried by people, either on their person or in bags, in mass transit and large crowd event venues. This type of parametric study and testing had not previously been undertaken in the global detection canine community. S&T has taken the lead to conduct this type of parametric study and testing, which is critical to understanding the limits of performance for the canine detection teams in these types of search applications.

Chairman Donovan, Chairman Katko, Ranking Member Payne, Ranking Member Watson Coleman, and distinguished Members of the committees, thank you again for your attention to this important mission and for the opportunity to discuss S&T's support to TSA and surface transportation agencies. I look forward to answering your questions.

Mr. KATKO. Thank you, Mr. Roberts.

Our fourth witness is Mr. Brian Michael Jenkins. In his role as director of the National Transportation Security Center of Excellence at the Mineta Transportation Institute, Mr. Jenkins directs continuing research on protecting surface transportation against terrorist attacks.

In 1996, President Clinton appointed Mr. Jenkins to the White House Commission on Aviation Safety and Security. From 1999 to 2000, he served as advisor to the National Commission on Terrorism and, in 2000, was appointed to U.S. Comptroller General's Advisory Board.

Mr. Jenkins is a decorated combat veteran, having served in the 7th Special Forces Group in the Dominican Republic and with a 5th Special Forces Group in Vietnam.

Sir, thank you for your extended service to our country, and the Chair now recognizes you for your opening statement.

STATEMENT OF BRIAN MICHAEL JENKINS, DIRECTOR, NATIONAL TRANSPORTATION SECURITY CENTER OF EXCELLENCE, MINETA TRANSPORTATION INSTITUTE

Mr. JENKINS. Chairman Katko, Donovan, Ranking Members Watson Coleman and Payne, distinguished Members of the committee, thank you very much for inviting me to testify.

Just yesterday, Homeland Security Secretary Nielsen underscored that America is at war, her words, with jihadist terrorists world-wide who continue to direct, assist, and inspire attacks here in the United States. Let me talk for a minute about the threat.

Terrorists see trains, transit systems, and buses as killing fields where most of their attacks are intended to cause large-scale casualties. Over the past 20 years, the Mineta Transportation Institute has maintained a database of what are now more than 5,000 attacks on surface transportation. Let me go to that database and give you some numbers.

Since 9/11, there have been nearly 3,000 attacks on surface transportation world-wide, resulting in more than 7,500 deaths; 14 of those attacks resulted in 50 or more fatalities each. If you just take those numbers, the 50 or more incidents, then that gives you something between 6 and 18 airline crashes or full hull losses.

In the United States alone, since 9/11, there have been 80 jihadist plots against all targets, more than 20 jihadist attacks.

Surface transportation was targeted in 2 attacks and in 10 separate terrorist plots.

World-wide, bombings, armed assaults, derailments lead the list on terrorist attacks on surface transportation. Bombings account for 58 percent of all the attacks and 51 percent of the fatalities; armed assaults, 11 percent; derailments, 8 percent.

In 2017, both al-Qaeda and ISIS encouraged followers to derail trains. This is a long-time ambition of Osama bin Laden, and al-Qaeda went further and provided on-line advice on how to build a concrete derailment device.

We haven't seen any noticeable increase in the number of attempted derailments overall, but just last week, a TGV high-speed train in France hit a concrete block placed on the rail line. It stopped the train. It did not derail the train. The incident is now being investigated.

Although, strictly speaking, not an attack on surface transportation, we do see an increase in vehicular assaults or car rammings. This is becoming a world-wide trend. There were 10 incidents between 1996 and 2013, but the pace has quickened since then. In the 4 years since 2014, there have been 40 such attacks, 20 in 2017 alone. The United States has experienced 6 of these attacks since 2006.

Analysis of foiled terrorist plots gives us some indications of how adversaries look at security. They avoid protected targets. They are aware of CCTV. The visible presence of police and other security personnel affects their planning. Over the long run, we can discern deterrent effects.

Finally, and this is good news, "If you see something, say something" campaigns work, and the rate of reporting is increasing. Reports of suspicious activity or suspicious objects by alert staff and passengers have resulted in authorities being able to thwart 11 percent of the attacks and find and disarm 20 percent of the bombs. That is a significant achievement. We might want to try to explore how we can improve public engagement even more. Thank you very much.

[The prepared statement of Mr. Jenkins follows:]

PREPARED STATEMENT OF BRIAN MICHAEL JENKINS[1]

JANUARY 29, 2018

Chairman Katko, Chairman Donovan, Ranking Members Watson Coleman and Payne, and distinguished Members of the Homeland Security Committee, thank you for inviting me to testify on the important topic of surface transportation security.

Public surface transportation offers terrorist attackers crowds of people concentrated in easily accessible (and escapable) venues. While sabotaging railroad tracks and other right-of-way infrastructure often may be intended as merely disruptive, terrorists see trains, transit systems, and buses as killing fields where attacks are intended to result in large-scale casualties.

Over the past 20 years, the Mineta Transportation Institute (MTI) has built and updated a detailed database that now contains more than 5,000 attacks on public surface transportation (primarily buses, trains, stations, and passenger ferries) since 1970. This database, which supports the Transportation Security Administration's (TSA's) analysis, as well as MTI's own reporting, provides a basis for assessing patterns and trends in terrorist tactics, targeting, and techniques.

[1] Jenkins is also the senior adviser to the president of the RAND Corporation.

My remarks today are largely based on observations from this database. I will focus on the terrorist threat and therefore the relevance of the proposed security measures.

Just yesterday, Secretary of Homeland Security Nielsen underlined that "America is at war" with jihadists world-wide who continue to direct, assist, and inspire attacks. She went on to say that the United States had seen a spike in terrorist attacks and that terrorist were increasingly targeting soft targets which have to be hardened.

Terrorist attacks on aviation have declined, although some terrorist groups remain fixated on sabotaging airliners, attacks targeting public surface transportation have increased. However, the shift from airlines to trains and buses and the underlying reasons are more complex than mere target substitution. Since 9/11, there have been 27 attacks (hijackings and sabotage attempts) on airliners and 110 attacks on airports. Attacking airports instead of airliners may be target substitution. Attacks on airliners resulted in 496 fatalities, while attacks on airports resulted in 195.

During the same period, 2,828 attacks targeted public surface transportation targets, (not including infrastructure) resulting in 7,524 deaths. That is an average of about 3 fatalities per attack, but it is noteworthy that 14 attacks resulted in 50 or more fatalities each. These are roughly equivalent to 6 "hull losses" or airline crashes. Examples include the 2004 Madrid commuter train bombing, which left 191 dead; the 2005 London transport bombings, which killed 52; and the 2007 Mumbai train bombing, in which 207 were killed.

Since 1970 the majority of attacks on surface transportation have taken place in developing countries, which have experienced approximately 4,500 such attacks. These attacks also are more lethal than attacks elsewhere. Europe has experienced 492 attacks since 1970, and the United States and Canada together have suffered 65 attacks, almost half of which were directed against passenger trains, stations, and buses. However, since 9/11, more than 80 terrorist plots against all target categories have been uncovered in the United States, along with more than 21 attacks inspired by jihadist ideology, and surface transportation has figured prominently in their plans.

Law enforcement authorities in the United States have done remarkably well in intercepting terrorist plots. Between 9/11 and 2017, the FBI, working with local police, uncovered and thwarted about 80 percent of all home-grown jihadist plots, often through undercover operations.[2] These plots provide a window into terrorist targeting preferences—and surface transportation features prominently.

Since 9/11, two surface transportation attacks were actually attempted. In October 2017, an armed white supremacist entered a secure area of an Amtrak passenger train engine and triggered an emergency stop. He was overpowered by train personnel and held for arrest; his ultimate intentions are not known. In December 2017, Akayed Ullah, inspired by ISIS ideology, detonated a crude pipe bomb attached to his body at a busy bus terminal in New York City. The device malfunctioned, injuring only the bomber.

Surface transportation targets were identified by terrorists in at least 10 additional reported terrorist plots in the United States. Canadian police also arrested two men charged with plotting to derail a passenger train between Toronto and New York. In addition to these plots, at least one terrorist attack and several shootings by mentally unstable individuals occurred in the public areas of airports.

Few of these interrupted plots reflected mature operational plans. As indicated, only two terrorists succeeded in making an actual attempt on surface transportation targets, and they achieved little result. Several plots were police "stings," in which the perpetrators identified the transportation targets. However, at least one plot, a planned multiple-attacker suicide bombing in New York in 2009, can be considered a close call. The plot's leader, who had trained in Afghanistan, reportedly had built suicide vests but destroyed them when he suspected police were about to close in. Collectively, the many plots indicate continued terrorist interest in targeting surface transportation.

Fortunately, America's post-9/11 cohort of home-grown terrorists have not proved to be especially competent. Their plots, for the most part, can be described as aspirational. Their desire to belong exceeds their concerns about their own security and they end up joining what turns out to be the "FBI branch" of al-Qaeda or ISIS. Their bombs seldom work. In two of four bombing attacks, the device did not detonate as expected. In the third attack—the Boston Marathon bombing—the terrorists' two bombs killed 3 persons, although many were injured. In a fourth jihadist

[2] Brian Michael Jenkins, *The Origins of America's Jihadists*, Santa Monica, Calif.: RAND Corporation, 2017.

attack involving bombs in New Jersey and New York, 20 were injured, none were killed. This gives U.S. Jihadist bombers an FPA (fatalities per attack) that is only a fraction of the world average.[3] Most jihadist terrorist bombings in the United States are one-offs—there is no learning and no improvement in skills.

Through their on-line publications, jihadist terrorist groups have urged followers to attack transportation systems. In 2017, both al-Qaeda and the Islamic State of Iraq and al-Sham (ISIS) encouraged attempts to derail trains, a long-time ambition of Osama bin Laden. Al-Qaeda in the Arabian Peninsula (AQAP) added to its exhortation instructions on how to build a derailing device. Thus far, there has been no noticeable increase in attacks aimed at derailment, however, on Sunday, January 21, a TGV high-speed train hit a concrete block placed on the rail line in the south of France. Two other blocks reportedly had been placed on the tracks. The train did not derail. French authorities are currently investigating whether there is a nexus to terrorism.

While terrorists have traditionally attacked unprotected targets, they have historically preferred venues with some symbolic importance. That is less and less the case as terrorists move toward what might be called "pure terrorism," attacking assemblies of people or individuals anywhere, killing simply to participate in bloodshed and make the point that no one is safe anywhere. ISIS, in particular, has attracted self-selecting terrorists whom it encourages with the promise of applause and ex post facto membership.

Bombings, armed assaults, and derailments lead the list of tactics employed against surface transportation world-wide, accounting for approximately 77 percent of all types of attacks and 74 percent of all fatalities. Bombings account for approximately 58 percent of attacks and 51 percent of fatalities. Armed assaults are individually more lethal. They account for about 11 percent of all attacks and 18 percent of all fatalities. We also see a growing number of primitive attacks involving knives and hatchets. Derailments, using bombs or mechanical means of sabotage, constitute almost another 8 percent of all attacks and account for 5 percent of total fatalities.

Although vehicular attacks are not, strictly speaking, attacks on public surface transportation, they are increasingly employed by terrorists world-wide (and some vehicular assaults abroad have been directed against surface transportation targets, for example, driving cars into bus stops or buses).[4] Both al-Qaeda and, more recently, ISIS have urged their followers to drive into crowds of pedestrians. A deadly vehicle attack took place in New York in October 2017, when an individual inspired by ISIS veered a rented truck on to a bike path, killing 8 people. Ten such attacks took place between 1996 and 2013, but since 2014, the pace has quickened, with more than 40 vehicular assaults. More than 20 of them occurred in 2017 alone. More than 150 people have been killed by homicidal drivers in the past 19 months, and nearly 800 have been injured. Seven such attacks have occurred in the United States since 2006. Vehicular assaults pose a major problem for urban planners.[5]

It is difficult to assess the effectiveness of security measures against terrorism. Terrorist attacks are statistically rare and random—there are too few, and they are spread over too many target categories and countries to allow empirical evaluation. Moreover, security measures don't "catch" would-be attackers like insects in a net. Few attacks are visibly prevented by security.[6]

Nevertheless, it is possible in some cases to discern deterrent effects. For example, as security to protect commercial aviation has increased over the years, there has been a corresponding decline in the number of attempted airline hijackings and bombings. A majority of these since 9/11 have involved mentally unbalanced individuals who, in fact, smuggled no weapons or explosive devices on board, but claimed to possess bombs. By the nature of their mental condition, they would not be easily deterred. Finally, most of the recent events have occurred outside of the United States and Europe, in places where security is less stringent. All of this suggests that deterrence has been effective.[7]

Analysis of foiled terrorist plots, in which apprehended terrorists were questioned about their target choices and planning considerations, has provided some indica-

---

[3] All statistics derive from MTI's database.

[4] Brian Michael Jenkins and Bruce R. Butterworth, *Terrorist Vehicle Attacks on Public Surface Transportation Targets*, San Jose, Calif.: Mineta Transportation Institute, 2017.

[5] Brian Michael Jenkins, "Navigating the Latest Terrorist Trend," U.S. News & World Report, December 19, 2017.

[6] Brian Michael Jenkins, *The Challenge of Protecting Transit and Passenger Rail*, San Jose, Calif.: Mineta Transportation Institute, 2017.

[7] Brian Michael Jenkins and Bruce R. Butterworth, *The Threat to Air and Ground Transportation Posed by Mentally Disordered Assailant*, San Jose, Calif.: Mineta Transportation Institute, 2017.

tions of how adversaries evaluate security measures. Terrorists demonstrably favor soft targets where they do not have to penetrate protected perimeters and are unlikely to encounter armed guards. There are ample public spaces that meet these criteria. Anecdotally, we know that terrorists are sometimes aware of CCTV and may try to disguise their reconnaissance efforts. The visible presence of police and other security personnel has caused them to delay attacks.[8]

The terrorists may presume that some kind of surveillance is in place—for example, the presumption of undercover police adds to uncertainty, which adversaries generally abhor. This suggests that robust security presence operating in unpredictable ways, accompanied by the impression that more security personnel might be present, contributes to deterrence, although the actual effect cannot be calculated.

One aspect of security merits further examination and effort. "See something, say something" works and the rate of reporting has been increasing. Observations and reports of suspicious activities or objects by employees, passengers, or others have enabled authorities to prevent 11 percent of terrorist attacks and to disarm or destroy 20 percent of terrorist bombs. Public education programs and intensified campaigns to engage staff and passengers may be able to further improve this performance.

Mr. KATKO. Thank you very much, Mr. Jenkins. We appreciate you being here today.

I now recognize myself for 5 minutes of questions—or actually what we are going to do is we will go to 3 minutes of questions, and then we are going to have to break very soon for votes, and then we are going to have to come back and get through it. So my question will be very brief, I hope.

We recently had a hearing on TSA's strategic 5-year technology investment plan. The purpose of that plan is to accelerate significant advancements in security technology capabilities and deployment of these systems in the Nation's TSA arena.

What is starkly lacking from that 5-year plan is any mention of surface transportation anywhere. So my question to you is: How would you describe TSA's prioritization of surface transportation capability gaps compared to aviation capability gaps? Anyone want to take that?

Mr. PRYOR. Yes, sir. I am the sacrificial technologist today.

Mr. KATKO. I guess the point is—I am not trying to put anybody on the spot here. To me, that is a glaring omission. I mean, we just had the first suicide—attempted suicide bombing of an American train system, and that is a pretty serious thing, and so that the 5-year technology plan is designed to force TSA to look at the advancing technologies.

Let me ask you this: Isn't it fair to say that it would be a good idea to have something in the 5-year technology plan regarding surface transportation systems?

Mr. PRYOR. Yes, sir. The 5-year technology plan is primarily focused on TSA's procurements through those 5 years, and as mentioned, TSA does not procure technologies directly for surface transportation venues.

TSA does have other plans—for example, the National Security Plan, the National Infrastructure Protection Plan, and others—that do talk about advancements in technology. As far as prioritization, TSA has many different priorities and has to rank order them according to TSA's understanding of its mission and its threats.

Mr. KATKO. I will just close with this, and I will move on, because I think it is only fair to give my colleagues a chance to ask.

---

[8] Brian Michael Jenkins, *Carnage Interrupted: An Analysis of Fifteen Terrorist Plots Against Public Surface Transportation*, San Jose, Calif. : Mineta Transportation Institute, 2012.

I will note that given the billions—with a B—the billions of passengers per year on American surface transportation systems, to me, it would be a good idea to start including that in part of the plan because, whether you like it or not, it is clear now that that is also a target of the bad guys, and so we should at least have something in there that forces public scrutiny in a more crystalized manner of that system.

So, with that, I recognize my colleague from New Jersey, Mrs. Watson Coleman, for questions.

Mrs. WATSON COLEMAN. Thank you very much, Mr. Chairman.

First, I would like to ask for unanimous consent to enter this letter in from the American Public Transportation Association in support of my legislation.

Mr. KATKO. Without objection, so ordered.

[The information follows:]

LETTER FROM THE AMERICAN PUBLIC TRANSPORTATION ASSOCIATION

DECEMBER 13, 2017.

The Honorable BONNIE WATSON COLEMAN,
United States House of Representatives, Washington, DC 20515.

DEAR CONGRESSWOMAN WATSON COLEMAN: On behalf of the more than 1,500 member organizations of the American Public Transportation Association (APTA) and the billions of public transportation riders across the nation, I thank you for your leadership in introducing the "Surface Transportation and Public Area Security Act of 2017."

The industry welcomes the bill's increased authorization for federal transit security funding. It would also improve intelligence information sharing and coordination and create new security training programs. Lastly, we appreciate the bill's provisions that promote research, demonstration, and implementation of innovative security technologies.

I thank you for the opportunity for APTA members to offer input on the bill. We look forward to working with you as the legislative process continues.

Sincerely,

RICHARD A. WHITE,
Acting President and CEO.

Mrs. WATSON COLEMAN. Thank you so much.

I am going to try to get some "yes" and "no"s here. So I am going to start with Ms. Proctor and anybody else that wants to jump in here.

I want to ask about: Do you believe that the security grants—the Transit Security Grants Program is effective?

Ms. PROCTOR. Yes, ma'am, I do.

Mrs. WATSON COLEMAN. Do you believe that it is undersourced? Do you think you need more money?

Ms. PROCTOR. I would say that the security partners that receive the grants would certainly agree with that.

Mrs. WATSON COLEMAN. Would certainly say so. What about the VIPR program? Do you think that that is helpful?

Ms. PROCTOR. The VIPR program has been a great asset to our security transportation partners in providing——

Mrs. WATSON COLEMAN. So do you support increasing the number of those? Do you think that that is a real link between security and—well, security?

Ms. PROCTOR. The presence of VIPR teams and surface transportation has true value.

Mrs. WATSON COLEMAN. What about just the additional canines as security? I am just so interested in them because I know that

the surface transportation issue is just so complex and so diverse that it seems to me that puppies trained are very helpful to keeping our passengers safe.

Ms. PROCTOR. I am certainly an advocate of the TSA canine program and believe it has great value in the surface transportation arena. You often see canines in places like Amtrak.

Mrs. WATSON COLEMAN. Yes.

Ms. PROCTOR. And WMATA.

Mrs. WATSON COLEMAN. So the answer is basically yes. I am sorry. I am just——

Ms. PROCTOR. Yes.

Mrs. WATSON COLEMAN. So, in addition to that, do you think that more law enforcement presence is a good deterrent as well and a good security measure?

Ms. PROCTOR. More law enforcement presence is always good.

Mrs. WATSON COLEMAN. Should I get you to sign an endorsement to my surface transportation legislation, which hopefully will be addressed? This is just a rhetorical question. I am not going to put you in that position.

Ms. PROCTOR. Thank you.

Mrs. WATSON COLEMAN. But it does address those needs that we think that are woefully inadequately addressed by TSA that is doing a yeoman's job in aviation but leaves a lot to be concerned about with regard to surface transportation.

I have a number of questions. I certainly would love to have a conversation with Mr. Jenkins about the fact that we don't have the experiences that other countries have had, and were there things that they do or can do with technology that they have that we don't have and don't employ and don't use, but I think my time has run out. But I would like you to put that in your mind, and if we can't get to that today, you will be able to give that some thought and communicate to us through the Chairman.

Mr. KATKO. I think—I am sorry. Thank you, Mrs. Watson Coleman.

I think we will have time after votes to revisit that issue.

Mrs. WATSON COLEMAN. OK.

Mr. KATKO. We will do another round of questioning so long as time permits.

Mrs. WATSON COLEMAN. I yield back.

Mr. KATKO. The Chair now recognizes the gentleman from New York, Mr. Donovan.

Mr. DONOVAN. We only have two votes, so we will be back real quick, so let me ask one question, and then we will get to the other stuff.

Mr. Roberts, I just wanted to ask you: The Surface Explosive Transportation Detection Program was created about 5 years ago, 6 years ago, in 2011, I believe it was. It was supposed to develop multi-layer detection systems. I was just wondering, have we deployed any of those, and if we have, how many, and if you at some point can provide a list for us?

Mr. ROBERTS. Yes, sir. The program began with cooperation of our customer component here, the TSA, and it began in basically a survey of the requirements needed. So the first couple of years was assessing whether what the end-users needed, what kind of

technology would work within their systems in a high-throughput open system. It also measured the concern with cost for these systems.

Then we developed a requirements pathway in our current technology development road map for these systems. So these current systems, we support TSA in developing technology to a developmental test and evaluation stage, proof of principle, and then we hand it off to Bob's mass transit test beds to be able to go through operational testing.

So we are still in the proof of principle stage with these multilayered sensor systems, and so we are not in the operational testing yet. We are in the developmental testing phase.

Mr. DONOVAN. Great. Thank you.

Mr. Chairman, I yield so we can get up to votes.

Mr. KATKO. Thank you, Mr. Donovan. The Chair now recognizes Mr. Payne for questioning.

Mr. PAYNE. Thank you. Mr. Proctor, last year, there were reports that Australian officials arrested two men last year trying to use an improvised chemical dispersion device to release a toxic chemical in public transportation. How is TSA working with its partners and offices and components at DHS to help transit owners and operators prevent, detect, and respond to similar threats?

Ms. PROCTOR. Thank you, Ranking Member. TSA has convened a number of opportunities to share this information with our stakeholders. We provided a Classified briefing of that threat to our mass transit and passenger security partners. We have held a workshop, a chemical threat workshop, to talk about some of the technological options that are out there. We did that in December.

We have shared information about countermeasures, and we continue to have that discussion with our security partners as we continue to plan training that will help them continue to train their work force.

Mr. PAYNE. OK. Thank you.

I yield back.

Mr. KATKO. Thank you, Mr. Payne.

This subcommittee hearing now stands in recess, subject to the call of the Chair, and I will caution everyone to please come back quickly right after the votes, and we will get right back at it. Thank you very much.

[Recess.]

Mr. KATKO. The hearing is now in session. Thank you for waiting for us in that delay. We got back as quickly as possible.

The Chair now recognizes from gentleman from Louisiana, Mr. Higgins, for 3 minutes of questioning.

Mr. HIGGINS. Thank you, Mr. Chairman. I will move quickly.

Madam, gentlemen, I represent the Third District of Louisiana, which is recognized as a hub of industrial growth in the petrochemical industry and oil and gas. Over $120 billion worth of projects either currently producing and under construction and expansion or moving quickly toward production and under construction. Each of these private-endeavor projects have stood up quite extensive security measures within their perimeters. They have excellent teams, including tactical teams from my friends at the thin

blue line. They have excellent screening of personnel for drugs and explosives regarding keeping that stuff off of the premises.

But I am concerned about—and I would like to hear your input on—the rural areas of rail systems and what are we doing to help secure these rail systems? These products—dangerous chemicals and fuels are leaving these projects, right, leaving these plants. They are either shipped by truck or by rail mostly. But the truck driver himself becomes a security asset because it is a single unit moving; he is driving it; he is responsible for it; and they accelerate quickly when they have left the security environment of the plant itself.

But, by rail, these—the railways—the trains exit very slowly. It takes them awhile to get up to speed. So I am concerned about a timed device, an explosive device, or a remotely-controlled device being placed on a slow-moving train carrying dangerous products through rural areas, because they don't stay in rural areas. They leave the plants. They go through heavily-populated areas and then onto their final destination. So what are we doing to help with that?

Mr. PRYOR. Thank you, sir. Technologically-wise, and of course, Chief Proctor has numbers of operational solutions as well, we are doing three general separate things. The first thing, we have a partnership with a major pipeline company—it would be a name you know, sir; I prefer not to give it in open session—where we provide infrastructure protection test bed for block valve sites, booster sites, and we have also put a small test bed up on the campus of our analysis laboratory, Johns Hopkins Applied Physics, up in Maryland, that they can use as a local prototype, and then we export those technologies. So that is the work we are doing in the physical plant.

In the case of rail, TSA led an effort a number of years ago that led to a redesign in tank cars to make them less susceptible to ballistic damage from high-powered rifles, 50-cals, those kinds of things, as well as the IEDs you mentioned. Those are rapidly coming into service. We also have pretty much pioneered within the United States under-vehicle screening systems. S&T collaborated with us, and those systems have actively been used in places like New York and others. So that is a third approach.

Then we also have a good understanding of ways that hazmat vehicles could potentially be controlled. If a shipper or a truck operator decides that they feel they have a threat, there are modifications that can be made to the vehicle to allow it to be safely disabled without harm to the driver or the public.

Mr. HIGGINS. Thank you for that very thorough answer.

Mr. Chairman, perhaps the members of the panel that have additional responses to my question could submit their answers in writing.

In the interest of time, I yield back.

Mr. KATKO. Thank you, Mr. Higgins.

Mr. HIGGINS. Thank you.

Mr. KATKO. The Chair recognizes the gentleman from Rhode Island, Mr. Langevin, for 3 minutes of questions.

Mr. LANGEVIN. Thank you, Mr. Chairman.

I want to thank our witnesses for being here today.

Mr. Chairman, as the panel's testimony has made very clear, countless Americans and American businesses depend on surface transportation every day, highlighting the importance of this hearing this afternoon.

So, increasingly, surface transportation providers rely on interconnected systems to monitor and control vehicles in supporting infrastructure. Now, with that increased connectivity, though, comes an increased responsibility to protect those systems against things like cyber threats. So recent events, including the ransomware attacks last June that debilitated several shipping and logistics companies in an incident reported just last week targeting a regional surface transportation provider in Toronto demonstrate that this threat is real.

So my question to start with, Ms. Proctor, in your testimony, you also discussed resources TSA invests to help surface owners and operators identify vulnerabilities and risks in their operations and to help owners and operators develop risk-mitigation solutions. So I want to know: Does TSA currently view cybersecurity as a capability gap in surface transportation security?

Ms. PROCTOR. Thank you so much for that question. Yes, sir. TSA does view cybersecurity as a gap. As you are aware, we have done a number of things to both educate our surface security partners on cybersecurity issues. We have developed tools for their use. We have developed the cybersecurity tool kit. We have started a number of cybersecurity workshops. We delivered 4 of those in fiscal year 2017. We have started a series of 6 in this fiscal year. Our focus in those is—those are focused on the nontechnical issues which end up really creating a lot of the problems with things like ransomware and phishing attacks.

So, in those workshops, we are focused on 5 things that they can do in their company. We call it 5 and 5. Five things you can do in 5 days that raise the cybersecurity bar in your company. When there are cyber-related incidents, we distribute cybersecurity awareness messages to our security partners to identify the threat and to encourage them to take certain steps so that they might be able to thwart future attempts.

We work very closely with ICS–CERT. We have worked very closely with them in developing, for instance, our pipeline security guidelines because of the significance of cyber in the control of the Nation's pipeline. So we have partnered with those that we realize are the recognized experts there in ICS–CERT, and we bring that knowledge to our surface security partners.

Mr. LANGEVIN. When you say "pipeline," does that include things like the supply chain?

Ms. PROCTOR. Yes, sir.

Mr. LANGEVIN. OK. Thank you. If I could, also, in your testimony, you described TSA's role in supporting the accurate and timely exchange of intelligence information with surface transportation owners and operators. So how does TSA monitor and share relevant intelligence about cybersecurity threats to the owners and operators of surface transportation systems?

Ms. PROCTOR. We provide briefings to our surface security partners. When appropriate, we provide Classified information to those cleared partners. But we provide that information through both

teleconferences, through our cybersecurity awareness messages, and through our work with ICS–CERT.

Mr. LANGEVIN. Thank you. I have gone over my time. I have some other questions I will submit for the record, but I want to thank our panel.

With that, I yield back.

Mr. KATKO. Thank you, Mr. Langevin. I will note that we are probably going to do a second round of 3 minutes of questions. If you want to stick around, we are happy to do so.

The Chair now recognizes the gentleman from Florida, Mr. Rutherford, for 3 minutes of questions.

Mr. RUTHERFORD. Thank you, Mr. Chairman.

Mr. Jenkins, in Mr. Roberts' testimony, he noted, and I quote: Public safety officials have little to no capability to detect threats being carried into surface transportation venues and must rely on intelligence reports before an attack.

You had some really good information, I think, about the types of attacks that have taken place against surface transportation. Seventy-seven percent of all attacks were bombing, armed assaults, or derailments, and then you went on to break that down. That is pretty good intel.

Has there been any kind of work with TSA to see that the nature of those attacks and then how we may be able to respond to those, besides the intelligence gathering that Mr. Roberts correctly pointed out is necessary?

Mr. JENKINS. The answer is yes. In fact, we maintain that database to support TSA. So we update the database every 15 days. TSA personnel and their intelligence folks and their analytical folks have the password that gives them direct access to the database. It is not available publicly.

Mr. RUTHERFORD. Uh-huh.

Mr. JENKINS. Because the database itself simply doesn't record the incident, it is a very detailed database that records, for example, if we are talking about explosives, method of delivery, method of concealment, type of explosives, and so on.

Mr. RUTHERFORD. Right.

Mr. JENKINS. TSA uses that to support their own analysis, and it supports, of course, at the same time, our separate reporting, and those reports go to TSA, and they go to the operators.

Mr. RUTHERFORD. OK. I understand, Ms. Proctor, that TSA is doing some work with stakeholders to get feedback on some testing and technology, but can you talk about any development of technology as a result of the information that has been provided, the kind of information that Mr. Jenkins is talking about? Are we utilizing that at ORCA or how——

Ms. PROCTOR. I would defer to Mr. Pryor on that question.

Mr. PRYOR. Yes, sir. Our annual work plans and spend plans rest on several fundamental analyses. One, of course, is threat and risk. Mr. Jenkins' information is always very helpful for us. Another one is on capability gaps provided by our industry partners. We have an annual process where those are developed. Then the third is National laws, 9/11 Act, National plans, and those sorts of things.

So risk is an important component of how we determine our work each year.

Mr. RUTHERFORD. Thank you, sir.

My time has run out. I yield back.

Mr. KATKO. Thank you, Mr. Rutherford.

I have two quick questions. The first one is something that I have been become aware of. It is a little off track here, a little bit but not much. I have become aware of the fact that it seems more and more that some train companies that haul hazardous material will oftentimes park those hazardous materials, sometimes for days on end, outside a secure area. I would like to hear if that is a growing concern amongst all of you, and whether that is an area of inquiry that we should get into, and whether or not you have concerns. Any of you?

Ms. PROCTOR. Mr. Chairman, the regulation requires that hazmat material on freight rail trains be maintained in a secure area. So they should not be left unattended in an area that is not considered secure. That is a requirement that they be in a secure area and maintained until they are transferred.

Mr. KATKO. I am aware what the regulations are, but I am asking—I guess I am asking, are you aware of instances where that is happening lately? That seems like this term single tracking comes to mind, where some companies engage in that, and, therefore, sometimes they are storing things outside of the secure area when they shouldn't be. Has that become an issue, or is that something that is not a big issue in your mind? Any of you? Anybody?

Ms. PROCTOR. Sir, that has not been something that has been brought to our attention. To the contrary, our surface inspectors report extremely high rate of compliance on that, so we have not had reports of that.

Mr. KATKO. OK. In a related matter, when you go through the cities—well, I will withdraw that. Let me change gears back to a more germane question here. There seems to be a pervasive, not just with TSA but Homeland Security as a whole, a prolonged technology development process. Sometimes by the time the technology gets to the front lines, it is already antiquated or on the way to being antiquated.

I would like to know from you all if there is any change to the TSIF for the testing facility that would help alleviate that process because there is a perceived bottleneck there. Are there things we could do with TSIF that might help that process? Anybody?

Mr. PRYOR. Yes, sir. TSIF is not a primary test venue for surface transportation. Its focus is primarily on passenger air. Because we are outwardly facing, we have a very adroit and high-speed process where we can induct products from industry, get them tested, and, if they are operation effective and suitable, put them in the field. That is one of the hallmarks of our program, and we do that through our relationships with many different laboratories and centers.

As I mentioned, our test lab is Applied Physics, but we also have relationships with Navy, DOD, a number of DOD agencies, Department of Energy, and others that allow us to leverage their developments to get things in the field for prototyping very quickly.

Mr. KATKO. Why aren't they doing it on the aviation side? Do you have any idea?

Mr. PRYOR. Procurement, of course, is managed by the Federal Acquisition and Regulations and other requirements, and the degree of rigor leading to a procurement often requires a significant amount of testing, particularly for passenger air. It is just in a different environment than the one we operate in where we have a great deal more flexibility in how we bring things to the field.

Mr. KATKO. All right. Thank you very much, very helpful.

I now recognize the gentlewoman from New Jersey, Mrs. Watson Coleman.

Mrs. WATSON COLEMAN. Thank you, Mr. Chairman.

Mr. Jenkins, I would like to have a conversation with you a little bit here. I am really concerned about the recent trend of terrorists who use trucks or cars or whatever, like in New York and like in Charlottesville. I am just wondering: These attacks, are these lone wolves, low financing, low planning, low everything? Is there anything that we should be doing, could be doing, that would make sense from a security perspective?

Mr. JENKINS. In terms of solving the problem as a security issue, it is limited. The fact is that, in cities, thousands, tens of thousands, millions of people live in close proximity, in some cases only inches away from thousands of vehicles. Without completely reconfiguring our urban landscape, we are not going to be able to create effective barriers throughout. We just have to be realistic about that.

Things that are being explored, I mean, everything from putting in place some barriers to protection of venues for certain periods of time that can be done, looking far out as we move toward more autonomous vehicles, then that may provide some solution in that they can be programmed not to do that. But, of course, that raises other kinds of cyber vulnerability. So this is one that we are simply going to be living with and struggling with. As I said, I am afraid, because, as you have correctly pointed out, it is so easy to do, that this is becoming a trend.

Mrs. WATSON COLEMAN. Thank you. We have been a bit more fortunate than places in Europe and otherwise as it relates to attacks on surface transportation. I am wondering: Do you know of any lessons that they have learned, any technologies they employ, any best practices they employ, having had these experiences, that we could be benefiting from if we had the resources? Is that kind of sharing happening?

Mr. JENKINS. First of all, there is coordination between what TSA does in terms of surface transportation and a great deal of liaison goes on between the other entities abroad, especially with the British, in terms of what they do for securing surface transportation. So there is a lot of exchange going on already.

In some cases, they have different approaches. For example, in France and in Belgium, either in response to intelligence or in response to a terrorist event, they will literally flood the transportation system with thousands of individuals drawn from the gendarmerie and drawn from the military, simply to augment security.

Mrs. WATSON COLEMAN. But this is related to intelligence, advance information, and——

Mr. JENKINS. Or an actual attack, and that is not an approach that we normally take.

Mrs. WATSON COLEMAN. We actually still haven't gotten to the other question that I had that I just want to put on the table, and that is, is there any technology that you see being employed in places that have had these experiences much more than us that would be helpful here? I will just be happy if you would send that information to me.

With that, I yield back. Thank you.

Mr. KATKO. Thank you, Mrs. Watson Coleman.

The Chair now recognizes the gentleman from New York for questioning.

Mr. DONOVAN. Thank you, Mr. Chairman.

Mr. Pryor, I think during the Chairman's questioning, you said that you are able to quickly deploy security measures that have been tested and get them out in the field as quickly as possible.

During your testimony earlier, Mr. Roberts, it has been 7 years now since the detection, multi-layer detection, has been authorized, has been in progress, and yet, 7 years later, we have nothing in the field. Can you explain to me what the obstacles are, and if so, what could be done about overcoming them?

The other part of my question would be: I suspect in those 7 years, our enemies, the people who are threatening our passengers, our riders, have changed their modes and their methods, and so we may be testing things that, in 2011, 2012, 2013, were their modes and methods, but now 6, 7 years later, those have changed, and maybe we are testing things that are obsolete now.

Mr. ROBERTS. Yes, sir. One of the things about the modes and methods—I will answer that portion first—is that, with Mr. Jenkins' report and with our international partners, we are aware of what the evolving threats are. So we are—our design points for our technology are still relevant and realistic.

As far as the 7-years piece, as I mentioned before, the first part of our program was standing up from nothing. We, along with our component customers, TSA, and our stakeholders, gathered and understood what the requirements were, what their priorities were. So what we did, in addition to that, is assess what was available as far as technology to stop this potential threat in an open system, high throughput, not interfering with existing infrastructure, those kinds of things. It was—we reviewed what was available in DOD and National laboratories, and Mr. Pryor's program tested and evaluated some of that. My program also did the same thing, the S&T program. So we started with the first piece of the program, just understanding where we needed to go and frame out the technology development pathway to set the requirements for our partners with the expertise.

So, really, where we are now in driving the technology development for our end goal started 2013, 2014, but it is—the testing and evaluation, it is not obsolete. It is designed with our end-users in mind. That is one of the reasons we are being successful in our technology development pathways; we are involving our component customers, as well as the stakeholders, in the design process.

Mr. DONOVAN. Even if that is true that it began in 2013, 2014, that is still 4 or 5 years ago. Do we have any expectations of getting anything in the field in the near future?

Mr. PRYOR. Sir, one part of your answer is that S&T and TSA occupy two separate parts of the mission space. S&T's job is to push the boundaries of technology, provide evolving technologies. TSA's part of the mission space is to take more advanced technologies, prototypes, things that will be entering in the marketplace soon, induct them, test them, give manufacturers improvements. So it is a continuum.

S&T will work for a few years, 3 or 4 or 5, to advance technology while we are operating in the marketplace, and then when their technologies are mature enough, they will transition them to us to actually assess.

Mr. DONOVAN. But none of the items that they have—and I am not criticizing their work; I am trying to figure out why it is such a long period of time—the things that they have tested, the technology that they have either proven to be workable or not workable, is still not in the field, it still hasn't been passed over to you to be put in the field yet? Am I understanding that correctly?

Mr. ROBERTS. Well, the program is framed out in near-, mid-, and far-term goals. Our near goals were video analytics to help these guys do, that are deployed currently, the FOVEA tool, at the Washington Metropolitan Area Center. So our near-term objectives and deliverables, the low-hanging fruit, for lack of a better word, is deployed now into the developmental testing realm and is near term with our operators.

The farther—the mid-term is automated detection of leave-behind bags. That is near-term. The further term is the harder problem: Detecting threats being brought in, either worn or carried in, in a high throughput open system. These are the longer-term goals as we establish the program, and they are about 3 to 5 years. Technology of this magnitude and for this hard problem is a long development time line.

Mr. DONOVAN. Three to 5 years, is that 3 to 5 years from the beginning or 3 to 5 years from now?

Mr. ROBERTS. Three to 5 years from now.

Mr. DONOVAN. Thank you.

I am way over my time, Mr. Chairman, I apologize.

Mr. KATKO. Not at all. Well, that concludes the hearing. I want to thank the witnesses for their thoughtful testimony and for discussing how TSA and S&T collaborate to address unique security threats facing transit systems.

To say the least, you are an impressive panel. You all have very impressive backgrounds, and we all thank you for the things you do to help keep this country safe.

I think in this time of increased threats—and we all know about them. We get briefed on a regular basis, and we see them on TV. The fact that we had the first attempted suicide bombing of a railway facility in the United States is a sober reminder of the ever-evolving threat.

So we need to be ever-vigilant, and we need to continue to work together, to continue to be a—need to conduct robust oversight of what you are doing, but we definitely need to get your information. It is impressive how much better the rail side is than the aviation side is about getting technologies to the front lines, and even on your side, it is still difficult, given some of the hurdles you need

to go through. So we are constantly trying to get past those hurdles to make sure that we give the front-line folks all the tools we have at our disposal. There is nothing more frustrating than seeing somebody with a good idea and that good idea never gets to front lines because of bureaucratic nonsense. That is something we are constantly fighting against.

So thank you all very much. You helped us and you helped us advance that cause.

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 VII(D), the hearing record will be held open for 10 days.

Without objection, the subcommittee stands adjourned. Thank you all.

[Whereupon, at 3:50 p.m., the subcommittees were adjourned.]