S. HRG. 115–651

SURFACE TRANSPORTATION SECURITY: ADDRESSING CURRENT AND EMERGING THREATS

HEARING

BEFORE THE

SUBCOMMITTEE ON SURFACE TRANSPORTATION AND MERCHANT MARINE INFRASTRUCTURE, SAFETY AND SECURITY

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JANUARY 23, 2018

Printed for the use of the Committee on Commerce, Science, and Transportation

Available online: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
37–297 PDF WASHINGTON : 2019

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JOHN THUNE, South Dakota, *Chairman*

ROGER F. WICKER, Mississippi
ROY BLUNT, Missouri
TED CRUZ, Texas
DEB FISCHER, Nebraska
JERRY MORAN, Kansas
DAN SULLIVAN, Alaska
DEAN HELLER, Nevada
JAMES INHOFE, Oklahoma
MIKE LEE, Utah
RON JOHNSON, Wisconsin
SHELLEY MOORE CAPITO, West Virginia
CORY GARDNER, Colorado
TODD YOUNG, Indiana

BILL NELSON, Florida, *Ranking*
MARIA CANTWELL, Washington
AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
EDWARD MARKEY, Massachusetts
TOM UDALL, New Mexico
GARY PETERS, Michigan
TAMMY BALDWIN, Wisconsin
TAMMY DUCKWORTH, Illinois
MAGGIE HASSAN, New Hampshire
CATHERINE CORTEZ MASTO, Nevada
JON TESTER, Montana

NICK ROSSI, *Staff Director*
ADRIAN ARNAKIS, *Deputy Staff Director*
JASON VAN BEEK, *General Counsel*
KIM LIPSKY, *Democratic Staff Director*
CHRIS DAY, *Democratic Deputy Staff Director*
RENAE BLACK, *Senior Counsel*

SUBCOMMITTEE ON SURFACE TRANSPORTATION AND MERCHANT MARINE INFRASTRUCTURE, SAFETY AND SECURITY

DEB FISCHER, Nebraska, *Chairman*
ROGER F. WICKER, Mississippi
ROY BLUNT, Missouri
DEAN HELLER, Nevada
JAMES INHOFE, Oklahoma
RON JOHNSON, Wisconsin
SHELLEY MOORE CAPITO, West Virginia
CORY GARDNER, Colorado
TODD YOUNG, Indiana

GARY PETERS, Michigan, *Ranking*
MARIA CANTWELL, Washington
AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, Connecticut
TOM UDALL, New Mexico
TAMMY BALDWIN, Wisconsin
TAMMY DUCKWORTH, Illinois
MAGGIE HASSAN, New Hampshire

CONTENTS

WITNESSES

APPENDIX

SURFACE TRANSPORTATION SECURITY: ADDRESSING CURRENT AND EMERGING THREATS

TUESDAY, JANUARY 23, 2018

U.S. SENATE,
SUBCOMMITTEE ON SURFACE TRANSPORTATION AND
MERCHANT MARINE INFRASTRUCTURE, SAFETY AND SECURITY,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:35 p.m., in room SR–253, Russell Senate Office Building, Hon. Deb Fischer, Chairman of the Subcommittee, presiding.

Present: Senators Fischer [presiding], Thune, Blunt, Johnson, Inhofe, Gardner, Young, Peters, Nelson, Cantwell, Klobuchar, Duckworth, Markey, Hassan, and Cortez Masto.

OPENING STATEMENT OF HON. DEB FISCHER, U.S. SENATOR FROM NEBRASKA

Senator FISCHER. The hearing will come to order.

I am pleased to convene the Senate Subcommittee on Surface Transportation and Merchant Marine Infrastructure, Safety and Security for our first hearing of 2018, titled "Surface Transportation Security: Addressing Current and Emerging Threats."

I also want to welcome Senator Peters, who is the new Ranking Member of this Subcommittee, and I look forward to working with him. A vote was just called. Senator Peters is voting and then will be coming up to the hearing. After I give my opening statement, I will be going to vote. Senator Inhofe will chair while I am gone, and then hopefully we'll have a pretty calm, good hearing following that.

We must ensure the security of all modes of transportation. This includes our roads, rail, ports, pipeline, and mass transit systems. Several recent and tragic incidents have highlighted the need for greater attention to transportation security.

In 2016, Europe saw terrible attacks that targeted transportation systems. In Nice, France, a member of ISIL drove a commercial truck into a crowded promenade, killing 84 people. Similarly, in March of that year, 16 people were killed in Brussels, Belgium, when a bomb detonated at a metro station.

The United States is not immune to these kinds of attacks. On December 11, 2017, a man detonated an improvised explosive device in an underground subway terminal in New York City. Thankfully, there were no fatalities, although three people did sustain in-

juries. A similar event occurred in New York City's Chelsea neighborhood in September 2016, when a terrorist used a bomb to injure 31 people near the town's train station.

These incidents are not exclusive to urban areas, either. Last October, an armed man was able to stop a California Zephyr Amtrak train near Oxford, Nebraska. He has since been charged with terrorism. We must be constantly vigilant against threats to our country, including on our Nation's transportation system. Al Qaeda has reportedly issued instructions for attacking our railroads, calling them our "easiest targets." It's clear that our ports, highways, pipelines, and railroads are at risk.

Today's hearing will focus on examining our response to threats to our surface transportation system. How we respond is vital to the security of passengers as well as our economic security.

The witnesses today oversee our transportation security system. On August 3, 2017, the Senate confirmed David Pekoske to be Administrator of the Transportation Security Administration. The Administrator previously served as Vice Commandant of the United States Coast Guard. We will also hear testimony from the Department of Homeland Security, Acting Inspector General John Kelly, who was appointed Deputy Inspector General in June 2016 and became Acting Inspector General in December 2017.

I thank you both for being here.

In examining our transportation system's security, we should examine the risks to our network as well as the resources TSA has to address those risks and counter potential attacks. The TSA does not directly manage surface transportation security the way it manages our airport security. Instead, TSA provides guidance, oversight, intelligence, and assistance to system operators and law enforcement as they work to secure our Nation's surface transportation network. This role is critical to close the gaps in our transportation security.

The men and women of TSA perform a tremendous service for our country, working night and day to keep passengers and freight secure. We must ensure TSA has the tools it needs to carry out its mission.

This Congress, I was proud to cosponsor the Surface and Maritime Transportation Security Act, a comprehensive bill to address gaps in our surface transportation security. For example, in September 2016, the Department of Homeland Security Inspector General found that TSA lacked an intelligence-driven, risk-based security strategy. Our bill would instruct TSA to implement a risk-based strategy so that it can more quickly and completely respond to those threats. It expands canine explosive detection teams, authorizes computer vetting systems for passenger railroads, and establishes a program to train surface transportation security operators and inspectors to identify and respond to threats. Additionally, it reforms the credentialing process for Transportation Worker Identification Credential, or TWIC, to ensure clarity with other credentialing programs. We will also examine the types of threats that face our transportation system, what strategies and technology are available to address these threats, and how TSA works with industry to shore up our security.

I look forward to the testimony of our witnesses.

And I would now like to invite our new Ranking Member of the Committee, Senator Peters, to the Subcommittee hearing. And if you would like to give your opening statement, sir.

STATEMENT OF HON. GARY PETERS,
U.S. SENATOR FROM MICHIGAN

Senator PETERS. Well, thank you, Madam Chair. And it's wonderful to be here with you. I'll look forward to working closely with you in the months and years ahead, hopefully.

Senator FISCHER. Good.

Senator PETERS. So. Well, thank you, again, Madam Chairman, for your—for holding this hearing on surface transportation today. I'm honored to work in this position, and look forward to delving into the issues that the Subcommittee has jurisdiction over.

Mr. Pekoske and Mr. Kelly, thank you both for your service to our country, and also thank you for being here today testifying before the Subcommittee.

I look forward to working closely with the Transportation Security Administration to ensure that the 60,000 public servants who are committed to keeping the traveling public safe have the tools and, equally as important, the resources to address the ongoing and emerging threats in the transportation sector.

As we have seen recently, surface transportation systems continue to be a target of terrorist attacks. Just last year, *Inspire,* an al Qaeda magazine, featured a cover story on how to derail trains, with the goal of wrecking or blowing up a train to create mass casualties. In December, a man carrying a pipe bomb attempted to detonate it in a crowded Port Authority bus terminal in New York City. And, tragically, we also saw, in New York City last year, how vehicles can be used effectively as weapons. In October, a man deliberately drove a rental truck down a bike path in Lower Manhattan, killing eight people and injuring 15 others. Abroad, we have, sadly, seen similar tragedies in England, Spain, Germany, and France. Vehicles have been used to cause injuries and casualties.

These attacks are an example of how quickly everyday life can be brought to a shocking and horrific halt. It's a reminder that we must find ways to address emerging threats and to better protect our citizens. And we've heard this call before.

We have known for years that our surface transportation system, particularly transit and rail, which attract large numbers of passengers, are particularly vulnerable. The 9/11 Commission, in 2004, recognized that rail and transit could be an attractive target for terrorists. And it's not just rail and transit. All types of surface transportation could be at risk. With thousands of containers moving in and out of ports, hazardous materials moving through pipelines, and cargo moving on trucks and rails across the country, the transportation network is vast as well as it is open. These systems still present a serious security challenge. A catastrophic failure to our transportation system could have serious economic consequences that impact every American.

We know this in Michigan, where an attack on line 5 pipeline in the Straits of Mackinac could cause significant environmental damage, or the Detroit Ambassador Bridge, which carries trade between the United States and Canada. So, we must ensure that the

Transportation Administration—the Security Administration is focusing its time and resources on developing and implementing new and innovative ways to adapt and meet the ever-changing threats to our transportation system.

That's why I joined with Chairman Thune, Ranking Member Nelson, Senator Fischer, and Senator Booker to support the Surface Transportation and Marine Security Act, which, as you know, passed this committee in April of last year. This bill will take a step to close the gaps in that security and provide additional resources to enhance security across our transportation system.

I look forward to hearing from our witnesses today on the actions that they have taken to adapt to security threats and what more we can do to secure our Nation's surface transportation system.

So, with that, Ranking Member Nelson, do you have comments?

STATEMENT OF HON. BILL NELSON,
U.S. SENATOR FROM FLORIDA

Senator NELSON. On behalf of the Committee and a lot of the things that Senator Peters has just mentioned, this Committee has considered and passed legislation to address it. For example, in 2016, we passed the Airport Security Enhancement Act. We took important steps to prevent insider threats to the aviation system. We increased random physical screenings and covert red-team testing. In addition, we have the TSA Modernization Act, which expands the use of explosives detection K9s, continues efforts to expand the TSA pre-check program, and extradites deployment of security screening technology.

And, while these steps are critical, but the threat is ever-changing. This is evidenced by TSA's announcement that the flights originating from the UAE, from Jordan, Saudi Arabia, Egypt, and Qatar to the U.S., will undergo enhanced cargo screening. And we have discussed previously in this Committee, I'm concerned that our current strategy does not address the vulnerabilities that we face today, including getting your technology, Mr. Administrator, using the very best technology for screenings of passengers. And so, we had that also, that attempted attack in the New York City transit station. We're going to have to address these deficiencies to secure all of these transportation systems.

So, I think it's time to reexamine our transportation security strategy and refocus our efforts.

And, with that, Mr. Chairman, I will conclude my opening comments.

[The prepared statement of Senator Nelson follows:]

PREPARED STATEMENT OF HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

I want to thank Chairman Fischer and Ranking Member Peters for holding this hearing about current and emerging threats to our Nation's surface transportation networks from terrorist attacks.

A series of attacks over the last year or so—from attacks in London and Barcelona to those right here in the U.S.—have rung the alarm bell. We cannot be content. Transportation remains a very real target for terrorists and those wishing to do harm.

This committee has heard that call. In 2016, we passed the Airport Security Enhancement and Oversight Act. In doing so, we took important steps to prevent insider threats to our aviation system. We increased random physical screenings and covert, red-team testing.

In addition, we have the TSA Modernization Act, which expands the use of explosive detection canines, continues efforts to expand the TSA PreCheck program and expedites deployment of security screening technology.

And while these steps are critical, the threat is ever changing. This is evidenced by the TSA's announcement that flights originating from the United Arab Emirates, Jordan, Saudi Arabia, Egypt and Qatar to the United States will undergo enhanced cargo screening.

As we have discussed previously in this committee, I am concerned that our current strategy does not address the vulnerabilities we face today.

Recent incidents and the attempted attack at the New York City transit station highlight the challenges we continue to face.

We must continue to address deficiencies to secure our rail, transit, port and freight transportation systems.

I believe it's time to reexamine our transportation security strategy and refocus our efforts.

We also need to provide sufficient funding to meet these challenges.

We cannot cut programs that help our communities prepare for and respond to threats.

And we need transit and port grants to help agencies improve their security infrastructure.

I want to thank the witnesses for coming today and I look forward to hearing from you on these issues.

STATEMENT OF HON. ROY BLUNT, U.S. SENATOR FROM MISSOURI

Senator BLUNT [presiding]. Well, thank you, Senator Nelson.

We're glad to have these witnesses with us today. David Pekoske, the Administrator of Transportation Security Administration, was sworn into that job last August. His previous work includes serving as the Vice Commandant of the U.S. Coast Guard and, in the private sector, supporting government counterterrorism and security services. John Kelly, the Acting Inspector General for the Department of Homeland Security, was appointed to his job in June 2016. He was appointed to his current role in December 2017. So, he's also new to this current job. But, his previous work includes service as the Deputy Assistant Inspector General for the Emergency Management and Oversight, as well as the Assistant Director for Forensic Audits and Special Investigations at GAO.

We're glad you're both here. And members will be returning from voting, but, Administrator Pekoske, if you want to go ahead and make your opening statement, followed by Mr. Kelly.

STATEMENT OF HON. DAVID P. PEKOSKE, ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Admiral PEKOSKE. Thank you, sir.

Chairwoman Fischer, Ranking Member Peters, and distinguished members of the Subcommittee, thank you for the opportunity to appear before you this afternoon alongside the Acting Inspector General.

Surface transportation security is a key priority of mine, and I'm looking forward to obtaining your perspective as we work together to address current and emerging threats.

First, let me acknowledge the outstanding men and women of TSA. It's my privilege to serve as Administrator to over 60,000 dedicated professionals. They provide security for millions of Americans who use our transportation systems each and every day.

Transportation security is an all-hands effort. Our aviation security checkpoint personnel are the most visible part of TSA, but there are thousands of other TSA employees working behind the scenes, in the air, around the globe, and with the owners and operators of our Nation's surface transportation systems. They all contribute to TSA's success and to our national security.

On behalf of this team, I thank you for your support in enabling TSA to accomplish a mission so critical to the safety, security, and economic well-being of the American people.

Madam Chairwoman, I have tremendous respect for the oversight role that this subcommittee performs. I highly value your perspective and opinions. You have made us stronger, and America safer. I appreciate the Subcommittee's work on the Surface and Maritime Transportation Security Act and the TSA Modernization Act.

Since becoming Administrator, I have spent a majority of my time at the front lines of TSA, engaging with TSA employees at all levels of the organization and meeting with our partners. Everywhere I have visited, I have found a deep commitment to the mission. That's so important, because, as you know, we face a determined adversary. The current threat environment is complex, diverse, and persistent, as illustrated by two recent terror attacks in the United States, the attempted suicide bombing in the Port Authority of New York and New Jersey bus terminal on December 11 that injured four people, including the bomber, and the vehicle ramming attack a few weeks earlier, on the west side of Manhattan, that killed eight people and injured 11. They both illustrate the risk our surface transportation systems are facing.

Unlike aviation, where TSA oversees and carries out day-to-day security operations in our Nation's airport, our role in surface transportation security is one of support, collaboration, and partnership with surface transportation owners and operators. The owners and operators, not TSA, are primarily responsible for their security operations. And we are proud of the partnerships we have developed, and the security improvements that have resulted from those partnerships.

While TSA's budget for surface transportation is small compared to the aviation sector, the Nation realizes a significant return from this investment when it is aligned, as it is, with the significant efforts being undertaken by our surface transportation partners. TSA's resources and personnel directly support ongoing security programs with committed security partners, who, in turn, dedicate millions of dollars to secure critical infrastructure, perform uniform law enforcement, public safety, and special security teams, and conduct regular operational activities and deterrence efforts.

The 9/11 Act placed 42 requirements on TSA. All have been completed, with the exception of three rulemakings. As I testified during my confirmation hearing, completing these rules is a top priority of mine, and I know it is a concern of yours. To update, a Notice of Proposed Rulemaking for security training was released in December 2016. The final rule is slated for publishing this coming summer as part of our DHS unified rulemaking agenda. An Advance Notice of Proposed Rulemaking for vulnerability assessments and security plans was also published in December 2016, and I ex-

pect this rule will proceed to the Notice of Proposed Rulemaking stage in Fiscal Year 2019. Finally, the rule on employee vetting is in the final drafting stages and will undergo DHS and OMB review this year. I expect a Notice of Proposed Rulemaking to be issued by the end of calendar year 2018.

It's important to note that, through the issuance of voluntary standards and guidelines developed collaboratively with industry, TSA has been able to effectively raise surface transportation security standards while the regulatory process proceeds. To support surface transportation owners and operators with their security needs, TSA focuses that—its efforts on regulatory oversight, system assessments, voluntary operator compliance with industry standards and TSA guidelines, collaborative law enforcement and security operations, accurate and timely exchange of intelligence information, intermodal training. And I'd note that we conduct intermodal security training and exercise programs, or called ISTEP programs, throughout the year, and we have a public area security summit scheduled for next month, here in Washington, D.C., dedicated to surface transportation security. Additionally, TSA performs technology development and testing. For example, we are testing a standoff person-borne IED detection system. This is in the final stages of operational testing and evaluation.

Chairwoman Fischer, Ranking Member Peters, and members of the Subcommittee, in closing, I am deeply committed to securing the U.S. transportation system from terrorist attacks. Thank you for the opportunity to testify today. And I look forward to your questions and comments.

[The prepared statement of Admiral Pekoske follows:]

PREPARED STATEMENT OF HON. DAVID P. PEKOSKE, ADMINISTRATOR,
TRANSPORTATION SECURITY ADMINISTRATION,
U.S. DEPARTMENT OF HOMELAND SECURITY

Good morning Chairman Fischer, Ranking Member Peters, and distinguished Members of the Committee. Thank you for inviting me here today to testify about the Transportation Security Administration's (TSA) role in surface transportation security.

My colleagues at TSA and I appreciate 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 I look forward to building on this relationship during my tenure at the helm of TSA.

The U.S. surface transportation system is a complex, interconnected network made up of mass transit systems, passenger and freight railroads, over-the-road bus operators, motor carrier operators, pipelines, and maritime facilities. These modes operate in close coordination with—and in proximity to—one another every day. To that point, the different modes of the surface transportation system often use the same roads, bridges, and tunnels to function. In short, the American economy and way of life depend on this network continuing to operate securely and safely.

To put the size of the system into perspective, consider that over 11 million passengers daily travel on the New York Metropolitan Transportation Authority (NY MTA) system alone. And more than 10 billion trips are taken each year on 6,800 U.S. mass transit systems, ranging from very small bus-only systems in rural areas to very large multi-modal systems, like the NY MTA, in urban areas. More than 500 individual freight railroads carrying essential goods operate on nearly 140,000 miles of track. Eight million large capacity commercial trucks and almost 4,000 commercial bus companies travel on the four 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. Over-the-road bus operators carry approximately 750 million intercity bus passengers each year. The pipeline system consists of approximately 3,000 private companies, which own and oper-

ate more than 2.5 million miles of pipelines transporting natural gas, refined petroleum products, and other commercial products.

As you can see, securing surface transportation is 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 an increase in vehicle ramming incidents around the world, including the most recent attack also in New York City—provide compelling reminders of the difficulty in securing a "system of systems" that is designed to quickly move massive volumes of passengers and commodities.

I look at three things when assessing risk in any particular transportation mode; the threat, the vulnerability, and the consequence, should an incident occur. When it comes to the surface mode, I take the threat very seriously. Because of the open nature of these systems, high ridership, and the types of commodities transported, the system is inherently vulnerable and the consequences of an attack would be high. 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. I am actively assessing how best to leverage and enhance TSA's surface expertise to strengthen our partnership with surface stakeholders.

TSA's Role

Unlike aviation, where TSA has been heavily involved in day-to-day security operations since its inception, surface transportation security has primarily been approached as a partnership with surface transportation owners and operators because they, not TSA, are primarily responsible for their own security operations. We believe this collaborative approach and relationship with surface owners and operators is appropriate. 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. TSA takes our security role for surface transportation very seriously. To best support surface transportation owners and operators with their security needs, we focus our efforts on system assessments, voluntary operator compliance with industry standards, collaborative law enforcement and security operations, accurate and timely exchange of intelligence information, and regulatory oversight. TSA's different role in security for surface transportation versus aviation is understandably reflected in its annual appropriation. Although TSA's budget for surface transportation is small compared to the aviation sector, the Nation realizes a significant return from this investment.

TSA's resources and personnel directly support ongoing security programs with committed security partners who, in turn, dedicate millions of dollars to secure critical infrastructure, provide uniformed law enforcement and specialty security teams, and conduct operational activities and deterrence efforts. TSA invests its resources to help those partners identify vulnerabilities and risks in their operations, and works with specific owners/operators to develop and implement risk-mitigating solutions to address their specific vulnerabilities and risks.

TSA is a co-Sector Specific Agency along with Department of Transportation (DOT) and United States Coast Guard (USCG) for the transportation sector. The USCG is the lead Federal agency for maritime security in the U.S., and TSA supports the USCG in its maritime security efforts and in coordinating interagency efforts for the maritime mode. DOT and TSA work collectively to integrate safety and security priorities for the other modes of surface transportation. Although DOT's regulations relate to safety, many safety activities and programs also benefit security and help to reduce overarching risk to the transportation system. In the surface environment, TSA has built upon those standards to improve the security posture with minimal regulations.

TSA's Approach

Information and intelligence sharing is at the heart of TSA's approach to surface transportation security. Whether we are providing unclassified information about known tactics, or classified information about specific threats, TSA works to deliver information to the appropriate surface transportation security partners. We maintain a communication network that facilitates the timely dissemination of information to stakeholders so they can take appropriate actions to prepare for, prevent and defeat acts of terrorism.

TSA also provides training and exercise support to surface transportation operators and their employees. The focus of those efforts is often on ensuring the effectiveness of communication channels, response plans, and other operational protocols. From frontline employees to security executives, TSA works to provide tools that en-

hance preparedness and close gaps in security planning. We host activities ranging from tabletop to full-scale exercises that focus on events associated with a single transit system to multi-modal regional events that bring federal, state, and local security and emergency response partners together.

Without the partnership, collaboration, and initiative of surface owners and operators, TSA could not fulfill our surface transportation security mission in making systems as safe and secure as practical. I have met with many representatives of the surface transportation community to better understand their concerns and perspective on securing the transportation network and continue to make this type of open dialogue a priority. To that end, TSA is hosting a Surface Public Area Security Summit next month to discuss security best practices and promote additional collaboration. This event will bring together domestic and international surface transportation stakeholders to discuss security challenges, various approaches to addressing them, and opportunities for future collaboration.

Innovation and technology

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. Partnership is the key to fostering innovation and ensuring the surface transportation system is secure both today and in the future.

TSA incorporates partner needs and capability gaps into our work to influence and stimulate the development of new security technologies in the marketplace. This effort is designed to make more readily available innovative and advanced technologies useful for public area security. We try to keep pace with the fast-moving advancement of security technologies to address current and evolving threats by looking at emerging technologies, including from outside the transportation environment, to determine applicability to the surface transportation environment. TSA works closely with surface transportation owners and operators to introduce new technology and approaches to securing surface transportation through 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. 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.

Implementing 9/11 Recommendations

We continue to work to address the remaining requirements of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act, Public Law 110–53). To date, TSA has met over 90 percent of the mandates imposed by the 9/11 Act, including 39 of the 42 surface transportation security-related mandates. Completing the remaining 9/11 Act requirements is among my highest priorities.

These mandates include the issuance of regulations for surface transportation employee training and vetting, the conducting of vulnerability assessments and standards for security plans, and mandates for the technology work just described. In December 2016, TSA issued the Notice of Proposed Rulemaking (NPRM) for the Surface Employee Training Rule and the Advance Notice of Proposed Rulemaking (ANPRM) for the Vulnerability Assessment and Security Plan Rule; TSA anticipates publication of the final Training Rule this Fiscal Year. While working on these rulemakings, TSA has taken steps through collaborative initiatives and assessments to ensure that front line employees receive security training and that owners and operators have robust security programs which include security plans, employee vetting and exercises.

Although the finalization of these rules is pending, TSA has worked diligently with stakeholders that would be affected by these rules to implement programs that meet, and in several instances exceed, what would be required by the rules. For example, TSA evaluates several areas required for a sound security program through our Baseline Assessment for Security Enhancement (BASE) program, including security training, security planning, and employee and contractor vetting. The majority of the higher-risk transit systems (those with daily passenger trips of 60,000 or higher) achieved a score of 90 percent or higher in the security planning, security training, and employee and contractor vetting areas in their most recent BASE reviews.

Conclusion

In closing, I believe a reinvigorated strategy is an essential foundation for success in our mission, and I have engaged my executive staff, with their years of experi-

ence, to reexamine and re-envision TSA's strategy and to place a much greater emphasis on surface transportation security—both in organizational and mission focus. I have also engaged many private sector surface transportation owners and operators to improve strategic partnerships and promote effective collaboration, and look forward to ongoing engagement with members of this committee as we develop our strategic path forward for TSA.

Chairman Fischer, Ranking Member Peters, and Members of the Committee, thank you for the opportunity to testify before you today. I am honored to serve in this capacity and I look forward to your questions.

Senator FISCHER [presiding]. Thank you, Administrator.

Mr. Kelly.

STATEMENT OF JOHN V. KELLY, ACTING INSPECTOR GENERAL, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. KELLY. Chairman Fischer, Ranking Member Peters, members of the Subcommittee, thank you for inviting me to testify alongside the TSA Administrator.

When the American public thinks of TSA, they think of a transportation security officer in a blue suit—or, I'm sorry, a blue shirt—instructing them to remove their belts and shoes before going through a security screening at an airport. The truth is that TSA has a much broader responsibility to also oversee and regulate our Nation's surface transportation modes, such as highways, freight, passenger rail, mass transit, and pipelines. Nevertheless, TSA dedicated only 2 percent of its 7-plus-billion-dollar budget on direct surface transportation expenditures.

In 2016, we were published—we published three reports that identified significant weaknesses in TSA's ability to secure surface transportation modes in the Nation's maritime facilities and vessels. Those reports identified a need for crosscutting, risk-based security strategy, the need for better controls in its background-check process, and delays in implementing passenger rail security regulations. My oral remarks highlight just a few of the key points from those reports.

First, TSA's strategy needs—or TSA needs a crosscutting, risk-based security strategy. In 2011, TSA began publicizing that it uses an intelligence-driven, risk-based approach for all transportation modes. However, we found that was not correct. In 2016, we reported that TSA specifically designed this approach only for air passenger screening. TSA has said it is working on a cross-country—crosscutting, risk-based strategy, but will not be available to provide it to us until April 2018.

As for the second report, TSA uses the Transportation Worker Identification Credential, or TWIC, to vet workers at our national ports and maritime facilities. The TWIC vetting process includes in immigration, criminal, and terrorism-related checks to identify offenses that could preclude someone from being granted unescorted access to secure facilities. Unfortunately, the TWIC vetting lacks key internal controls that compromise the program's reliability. These weaknesses leave our Nation's seaports at risk for terrorists, exploitation, smuggling, insider threats, and internal conspiracies.

Finally, TSA failed to develop and implement rail security regulations required by the 9/11 Act of 2007 that Congress passed 10 years ago. Surface transportation vulnerabilities can be best illustrated by the Ankara, Turkey, railway station bombing in 2015; the

Brussels, Belgium, metro bombing in 2016; and the St. Petersburg, Russia, metro bombing in 2017.

Passenger and freight rail and computer rail have unique security concerns. They operate in open infrastructures with multiple access points. That makes it impractical to subject all rail passengers to the type of screenings that air passengers undergo. Consequently, unlike TSA's security presence at airports, TSA's responsibility for rail passengers consists of assessing intelligence, sharing threat information with industry stakeholders, developing industry best practices, and enforcing regulations.

Notwithstanding these differences, TSA could have taken actions to strengthen rail security. Unfortunately, neither—TSA neither identified high-risk carriers nor issued regulations requiring those carriers to conduct vulnerability assessments and implement TSA-approved security plans. TSA also did not issue regulations that would require a railroad security training program and security background checks for front-line employees. Your Surface and Maritime Transportation Security Act addresses many of these issues.

Madam Chairman, this concludes my oral testimony. I welcome any questions that you or other members may—might have.

[The prepared statement of Mr. Kelly follows:]

PREPARED STATEMENT OF JOHN V. KELLY, ACTING INSPECTOR GENERAL, U.S. DEPARTMENT OF HOMELAND SECURITY

Chairman Fischer, Ranking Member Peters, and members of the Subcommittee, thank you for inviting me to testify at today's hearing regarding the security of our surface transportation security.

When the American public thinks of TSA, they think of the Transportation Security Officer in a blue shirt instructing them to remove their belts and shoes before going through security screening at the airport. The truth is that TSA has a much broader responsibility to also oversee and regulate our Nation's surface transportation modes—highway, freight and passenger rail, mass transit, and pipelines—to ensure the freedom of movement for people and commerce. Recent history—the October 2015 bombing of a railway station in Ankara, Turkey; the March 2016 metro bombing in Brussels, Belgium; and the April 2017 metro bombing in St. Petersburg, Russia—depicts how vulnerable surface transportation can be. However, TSA's budget reflects the public perception of its mission, allocating most of its resources to air passenger screening and dedicating only a small portion to these vulnerable areas of non-aviation.

In 2016, the OIG published three reports [1] that identify significant weaknesses in TSA's ability to secure surface transportation modes and the Nation's maritime facilities and vessels. Specifically, we identified issues with TSA's ability to identify risk across all modes of transportation, the reliability of background checks for port workers, and passenger rail security.

TSA Needs a Crosscutting Risk-Based Security Strategy

TSA has many responsibilities beyond air travel, and is responsible, generally through the use of regulation and oversight, for surface transportation security. However, TSA focuses primarily on air transportation security and largely ignores other modes. We found that TSA does not have an intelligence-driven, risk-based security strategy to inform security and budget needs across all types of transportation.

In 2011, TSA began publicizing that it uses an "intelligence-driven, risk-based approach" across all transportation modes. However, we found this not to be true. In an audit we released in September 2016, we reported that TSA specifically designed this approach to replace its one-size-fits-all approach to air passenger screening but did not apply it to other transportation modes.

[1] *TSA Oversight of National Passenger Rail System Security* (OIG–16–91); *TWIC Background Checks are Not as Reliable as They Could Be* (OIG–16–128); and *Transportation Security Administration Needs a Crosscutting Risk-Based Security Strategy* (OIG–16–134).

Additionally, TSA's agency-wide risk management organizations provide little oversight of TSA's surface transportation security programs. TSA established an Executive Risk Steering Committee charged with creating a crosscutting, risk-based strategy, which would drive resource allocations across all modes. However, neither it, nor any of these entities place much emphasis on non-air transportation modes.

In September 2017, TSA reported that it created a crosscutting risk-based strategy based on our recommendations and expected to finalize the strategy in October 2017. However, TSA did not submit this strategy to the OIG. Instead, in January 2018, TSA reported that it intends to submit its pending 2018 National Strategy for Transportation Security (NSTS) as its response to our recommendation for a crosscutting risk-based security strategy. The 2018 NSTS is due to Congress on April 1, 2018 and TSA expects to provide us with a copy by the same date.

We also reported that TSA lacked a formal process to incorporate risk into its budget formulation decisions. Despite the disparate requirements on the agency, TSA dedicated 80 percent of its nearly $7.4 billion FY 2015 budget to direct aviation security expenditures, and only about 2 percent to direct surface transportation expenditures. Its remaining resources were spent on support and intelligence functions. We recommended that TSA establish a formal budget planning process that uses risk to help inform resource allocations.

In September 2017, TSA provided documentation of the steps it has taken to establish a formal budget process that incorporates risk. This includes the development of a formal Planning, Programming, Budgeting, and Execution framework, standing up the Planning and Programming Analysis Branch, and creating five resource portfolios that, among other things, prioritize mission needs across the agency. However, we cannot close this recommendation until we receive TSA's risk-based security strategy and ensure that the strategy's guidelines for aligning resources with risk correspond with its new budget process.

TSA Missing Key Controls within the TWIC Background Check Process

TSA—responsible for safeguarding our Nation's ports and maritime facilities through the Transportation Worker Identification Credential (TWIC) program—lacks key internal controls and this compromises the TWIC program's reliability. These weaknesses leave our Nation's seaports at risk for terrorist exploitation, smuggling, insider threats, and internal conspiracies.

TSA provides background checks, or security threat assessments, for individuals who need unescorted access to secure port facilities; and issues a biometric identification card, also known as a TWIC. The background check process for TWICs is the same as that of aviation workers[2] and drivers who need a Hazmat Materials Endorsement.[3] It includes a check for immigration-, criminal-, and terrorism-related offenses that would preclude someone from being granted unescorted access to secure facilities at seaports.

In 2011, the Government Accountability Office (GAO) identified key internal control weaknesses in TSA's management of the TWIC background check process and recommended the Department take significant steps to improve the effectiveness of the program as a whole.[4] Although TSA took some steps to address GAO's concerns, our review—five years later—found that TSA did not adequately integrate the security measures intended to identify fraudulent applications into the background check process. For example, TSA required enrollment staff to use a digital scanner that could evaluate security features present on identification documents and generate a score to help TSA determine if the document was authentic. However, TSA did not collect or use these scores when completing its background checks—nullifying the effectiveness of this security measure. For those documents that could not be electronically scanned, TSA required the staff at the enrollment centers to manually review identity documents. However, TSA did not require that the staff be trained at detecting fraudulent documents. When the enrollment staff documented their observations of suspicious identity documents in TSA's system, TSA did not have a standardized process for collecting, reviewing, or using the notes when completing the background checks.

We determined TSA management's lack of oversight was the primary reason the TWIC background check process had many control weaknesses. At the time of our review, the TWIC background check process was divided among multiple program

---

[2] *TSA Can Improve Aviation Worker Vetting* (OIG–15–98)

[3] Commercial drivers required to transport hazardous materials must undergo a background check by TSA prior to receiving a hazardous material endorsement on their Commercial Driver's License.

[4] *Transportation Worker Identification Credential: Internal Control Weaknesses Need to be Corrected to Help Achieve Security Objectives* (GAO–11–657).

offices so that no single entity had complete oversight and authority over the program. In addition, the TWIC program lacked key metrics to measure TSA's success in achieving program core objectives. For example, the measures in place focused on customer service, such as enrollment time and help desk response time, rather than the accuracy of the background check itself.

As of November 2016, TSA realigned its operations and assigned the Assistant Administrator for the Office of Intelligence and Analysis as the single point of accountability within TSA for the TWIC program's management and operations with the functional oversight over all of the security threat assessment process.

Additionally, since our review, TSA completed a comprehensive risk analysis that reviewed existing controls, identified and analyzed risks, and promoted control activities. TSA is in the process of addressing the concerns identified by the study. TSA also updated its program charter and objectives to focus on (1) efforts to positively verify the identity of applicants; (2) conduct of the TSA Security Threat Assessment; and (3) actions to recurrently vet and revoke TWIC validity. TSA intends to update its performance metrics to better align with the revised objectives. We will continue to monitor TSA's progress in implementing corrective actions to strengthen the TWIC program.

TSA Delays Implementing Passenger Rail Security Regulations

TSA has failed to develop and implement regulations governing passenger rail security required more than nine years ago by the *Implementing Recommendations of the 9/11 Commission Act of 2007* (*9/11 Act*).[5] Unlike the security presence that TSA provides air passengers in airports, its responsibility for rail passengers rests in assessing intelligence, sharing threat information with industry stakeholders, developing industry best practices, and enforcing regulations. This is particularly important due to the volume of passengers using this mode of transportation and the unique challenges in the rail environment.

In Fiscal Year 2015 alone, Amtrak carried 31 million passengers across the continental United States and Canada, and operated more than 300 trains daily. Additionally, Amtrak and other passenger rail carriers operate in an open infrastructure with multiple access points that make it impractical to subject all rail passengers to the type of security screening that passengers undergo at airports. Notwithstanding this, there were actions that TSA could have taken, but did not, that would have strengthened rail security. Specifically, although required to by the *9/11 Act,* TSA neither identified high-risk carriers nor issued regulations requiring those carriers to conduct vulnerability assessments and implement DHS-approved security plans. TSA also did not issue regulations that would require a railroad security training program and security background checks for frontline employees. Regulations to implement a training program are important to ensure rail carriers have a mechanism in place to prepare rail employees for potential security threats.

Furthermore, unlike aviation and maritime port workers, TSA did not develop regulations requiring security background checks for rail workers. TSA vets airport and maritime port workers who need unescorted access to secure areas against the terrorist watchlist and immigration status and criminal history information, and these processes are consistent with the requirements in the *9/11 Act.*

These very issues were identified in 2009 by GAO, which reported that TSA had only completed one of the key passenger rail requirements from the *9/11 Act.* Seven years later, we identified that the same rail requirements—a regulation for rail carriers to complete security assessments, a regulation for rail security training, and a program for conducting background checks on rail employees—remain incomplete.

Following the 2004 terrorist attack on a passenger train in Madrid, Spain, TSA issued a security directive for Amtrak. That directive required carriers to improve security procedures by designating a rail security coordinator, reporting significant security concerns to TSA, and allowing TSA to conduct inspections for any potential security threats. TSA does conduct some limited inspections to verify carrier compliance with these requirements. However, TSA does not enforce other aspects of the security directive, such as the use of bomb-resistant trash receptacles, canine teams, rail car inspections, and passenger identification checks to enhance security and deter terrorist attacks. Instead, TSA relies on Amtrak and other transit entities to implement security measures if resources permit, and is even considering rescinding these minimal requirements from the directive. Without enforcing all security requirements, TSA diminishes the directives importance and carriers ability to prevent or deter acts of terrorism.

Since the issuance of our report in May 2016, TSA has taken steps to implement two of the three remaining requirements. TSA issued a Notice of Proposed Rule-

[5] Public Law 110–53.

making requiring security training for employees of higher-risk and anticipates a final rule by the end of the fiscal year. In the spring of 2018 TSA plans to issue a Notice of Proposed Rulemaking requiring security vetting for certain rail employees. TSA asserts that Executive Order 13771 (which establishes a requirement where an agency must eliminate two existing regulations for any new regulation the agency wishes to issue), is complicating the issuance of the agency's new rulemakings. If TSA does not fulfill these requirements, it cannot ensure that passenger rail carriers will implement security measures that may prevent or deter acts of terrorism.

Pending Legislation

Many of the issues I've discussed today are addressed in the S. 763, *Surface and Maritime Transportation Security Act.* I want to thank the Committee for introducing legislation to address a number of the challenges facing the Department. We believe that if enacted, this legislation will direct numerous improvements to our Nation's security. However, I must emphasize that the Department and TSA have demonstrated a pattern of being dismissive and lax on implementing requirements related to non-aviation security. Under these circumstances, change will require significant attention by Congress, the Inspector General, and the Comptroller General to ensure that TSA and the Department take timely actions to implement these improvements.

Future work

We will continue to audit and evaluate the Department's aviation and non-aviation-related programs, report our results, and closely track report recommendations. Currently, we are reviewing the effectiveness of access controls to secured airport areas; Federal Air Marshal Service international flight operations and ground-based assignments; TSA's efforts to hire, train, and retrain its employees; and TSA's use of the Sensitive Security Information designation. We are also planning reviews on the security of rail facilities; TSA's canine program; and a review of TWIC that is mandated by P.L. 114–244, *Essential Transportation Worker Identification Credential Assessment Act.*

Madame Chairman, this concludes my testimony. I welcome any questions you or any other members of the Subcommittee may have.

Senator FISCHER. Thank you very much.

We'll begin our first round of questions.

Mr. Kelly, as you noted in your testimony, TSA lacks an intelligence-driven, risk-based security strategy across all modes of transportation, and does not incorporate risk into its budgetary decision-making. So, what should be included in this strategy? And what effect do you expect incorporating risk into the TSA's budget formulation decisions will have on the agency's allocation of resources between all those different modes of transportation?

Mr. KELLY. To answer your second question first, I think there will be an increase in allocations toward surface transportation. While air transportation is very risky, I think the number of recent attacks on surface transportation areas are going to demonstrate that there's a much greater risk associated with surface transportation, and that there needs to be additional emphasis put in those areas.

Senator FISCHER. Administrator, can you give us, here on the Committee, an update on the work that you're doing to develop that risk-based security strategy so it does incorporate all modes of transportation?

Admiral PEKOSKE. Yes, ma'am. We're working on a national strategy for transportation security required by law. The two-year update is due on August 1 to the Congress. That's well in process. We're putting the final touches on that. That does embed a risk-based look across all modes.

The Acting IG is correct, when we talk about risk-based, it's only within the aviation sector, not across all the surface sectors. This national transportation security strategy will begin to do that.

Senator FISCHER. In previous hearings, I've tried to highlight my concern about the really very small percentage of TSA's resources that are dedicated to surface transportation responsibilities. What is your priority for surface transportation security? And do you have plans so that you can make adjustments to that allocation of resources?

Admiral PEKOSKE. Yes, ma'am. Our priority, we—you know, we have a very, very good partnership and working relationship with the owners and operators of surface transportation systems. And really our investment helps leverage the investments that they make all around the country. We've established several frameworks and a good set of guidelines across the different modes of surface transportation that our partners use really as their standards for performance. And so, while we don't have regulations in place in all cases, the guidelines we do have in place have allowed us to raise the bar, if you will, on surface transportation security.

I will look, as we look at developing our fiscal 2020 budget, so the—you know, I came into office in August. The fiscal 2019 budget was largely complete at that point. The fiscal 2020 budget begins its development over the next couple of months. We've already set up some initial standards, if you will, or guidance, for developing that fiscal 2020 budget. And, with that guidance, I—you know, I hope to use that risk-based approach to look at our allocation of resources to surface transportation across the modes of surface transportation, particularly as it relates to aviation security.

Senator FISCHER. If we look at other modes of transportation, though, besides aviation security for example, the Amtrak train that was attacked in the State of Nebraska in a very rural part of our state; a passenger train was attacked, and it has been determined it was a terrorist attack: how do you address that now? I know it would be very difficult, very costly to try to monitor all of rail across this country, let alone all of our highways, roads, city streets where these attacks can happen at any time. But, right now focus specifically on rail and how, or if, you work with Amtrak, how you coordinate on security to make sure that rail transportation is secure, please.

Admiral PEKOSKE. Yes, ma'am. We work very closely with Amtrak, and we have a program called Rail Safe, where Amtrak sponsors a—an exercise, where we bring in all the partners. Because, of course, Amtrak, as the—as the train moves down the rails, it impacts many, many jurisdictions and many other partners along the way. And so, these—that program has been very successful. Amtrak has done a very good job of training their employees. And Amtrak has a random process wherein they check baggage of their passengers and also the identity of their passengers.

But, it really goes to trying to work collaboratively with Amtrak and passenger rail, in general, because we provide an intelligence basis, due to our ability to query the U.S. intelligence community, and provide information to them. And so, a big part of our role is to ensure that we provide that information on a timely basis, and also look at best practices across other transportation modes. You

know, there may be a best practice in mass transit that might be very applicable to Amtrak, for example. And so, we work very hard to make sure we make those connections.

Senator FISCHER. And do you receive information on a fairly regular basis from our intelligence community?

Admiral PEKOSKE. We do. And we also have the ability to query the community. So, if Amtrak has a concern about a particular issue, we can query the community, and the community has been very responsive to those queries. For example, that issue that you raised with the magazine from ISIS that talked about ways to affect train travel in the United States. We, basically, went back to the intelligence community, asked them for their—that assessment, and provided that back to Amtrak.

Senator FISCHER. OK. Thank you, sir.

Senator Peters.

Senator PETERS. Thank you, Madam Chair.

And thank you, to our witnesses again, for being here today. Appreciate it.

I think it's fairly clear that the surface transportation system is at risk, and there's significant risk. And I outlined them—Chair, I, myself, outlined some of the attacks that the American public is very aware of. Mr. Pekoske, you mentioned them, as well, in your opening comments, as well. So—and these attacks aren't going to go away. If anything, we're seeing an escalation of them, as well. And more and more devastating, as well. But, despite these continued threats to our transportation system, President Trump's budget request would have significant cuts to what is already a small percentage of your budget. In fact, if I look at the President's budget, public transportation, rail and bus, about 100 million is spent now. That would be cut in half, roughly, to 48 million. Over half. While the risks are clearly going up, a cut of half. Ports, the same situation, 100 to 48. Surface programs, generally, from 122 to 86.

Mr. Pekoske, just give me a sense. We are already stretched, I believe. It's already a very small part of your budget. And then to now have to take budget cuts of roughly half to surface transportation, what is that going to mean to the safety of the American public?

Admiral PEKOSKE. Well, the cuts in the budget that you cite, sir, are cuts that are primarily directed at the Viper Teams, which are teams that we provide that provide a visible deterrent presence aboard surface transportation systems. It does not affect our communications, our collaboration, our establishment of guidelines, our training, our provision of intelligence information, our sponsorship of exercises, and things like that. But, the Viper reduction in the Fiscal Year 2018 budget was a big part of the reduction overall in surface transportation.

I'd also say, sir, that, in the budget, there's never enough there, for sure. And, as I look at the threats across the entire transportation spectrum, the threats to aviation are so significant and so prevalent. And I'm not minimizing in any way, shape, or form, the threats to surface, but we need to keep our focus there, as well. So, within a—if you look at the top line of TSA, that top line is not growing, it's shrinking, which requires some very hard decisions, in terms of how you fit into that top-line number.

Senator PETERS. Well, I think we all recognize that the aviation threat is significant. But, given the fact that—is it 2 percent for surface? Is—what I understand is, 2 percent of your budget goes for surface. And yet, a lot of the attacks that we have seen of late are really involved with surface transportation. I know you're in the process of doing a risk-based analysis as to how we prioritize. And that's just good management. And, obviously, we need to do be doing that. But, still, does it just make sense, in your professional capacity, that, really, is 98 percent of the risk in the aviation community, or do we need to be focusing more on increasing that 2 percent to the surface transportation area?

Admiral PEKOSKE. Yes, sir. I think, overall, the 2 percent—2 or 3 percent does need to go up, for sure. But, there is a major difference between what we provide in surface transportation, as far as security goes, and aviation. Because we actually provide the security in the aviation sector. So, a great proportion of the TSA workforce, all those salaries, all that training, all that support, is in the aviation sector because we actually directly provide the security there. So, it's kind of hard to compare the two from an absolute-dollars-to-absolute-dollars perspective.

Additionally, there's significant investment on the part of the owners and operators of these surface transportation systems, that, if you were to make that—try to make that direct comparison, you really would have to wrap in that investment, as well.

Senator PETERS. Mr. Kelly, in—your testimony included comments about TSA's lack of attention to surface security. And I read that very closely. Specifically, you warned that the TSA was dismissive and lacks on implementing requirements related to non-aviation security. If you could elaborate on that, and perhaps comment on Mr. Pekoske's testimony, as well, I'd appreciate it.

Mr. KELLY. Certainly. Out of the ten recommendations that were re-issued on the three reports that I referenced, only three of those recommendations have been closed. Those recommendations were made anywhere from 19 to 20 months ago. And it has been taking an extended period of time for them to implement those recommendations.

The three recommendations that they implemented were relatively easy to achieve, because it only required them to identify certain things or work within their own organization—didn't require them to move outside of TSA.

The—I will tell you, though, in working with the Administrator, my predecessor and I have noticed that he's very committed to improving the TSA, and he has only been on the job for less than 6 months, and attacking some of these issues are going to take extended working with his staff to actually implement them. So, I'm encouraged with his actions to move in the right direction.

Senator PETERS. Right. Thank you, Mr. Kelly.

Senator FISCHER. Thank you, Senator Peters.

We've been joined by the Ranking Member of the Committee.

Senator Nelson.

Senator NELSON. Thank you, Madam Chair.

What I want to talk to you about is the red team that went in to do a covert test. And, needless to say, the results were disappointing. So, what has TSA done to address the fact that huge

numbers of people got through TSA screening with weapons? And, further, how about the CT scanners? Talk about the next generation that would solve the problem.

Admiral PEKOSKE. Yes, sir. Let me start with the CT scanners first, because you can solve the problem by—in three ways: with technology, with a change in procedures, or a change in training. In my opinion, the technology piece is the one that will have, on the margin, the greatest impact on security effectiveness. And so, that's my clear focus for aviation security. We've stood up a project for—to begin to deploy CT technology to the checkpoints. We should begin to see some CT machines in checkpoints around the country for testing purposes this year. And we hope to complete the initial testing by the end of the summer, and then begin to deploy larger numbers of CT machines in Fiscal Year 2019. President's budget is due to be released on the fifth of February, and that will contain an investment on CT equipment at the checkpoint.

And also, sir, with respect to procedures, once we saw the intelligence information, examined the threats, and also had the benefit of the IG's covert testing results and our own covert testing results, we saw a need to change the procedures at our checkpoint. And so, many passengers, from August all the way through today, have noticed a change in procedures at the checkpoint, where we ask passengers to take more things out of their carry-on bags and put it in the bins. The reason for that is, it declutters the X-ray image for us, and makes the examination of the X-ray image much more effective. But, that's not the only part of that changed procedure. We also changed the procedure that our officers use to examine that X-ray image that we found to be much more effective, and the way we search the bags that we need to search. And so, overall, that procedural change, alone, in our own covert testing that is very akin to the IG's red-team testing, is an improvement of about 20 percent in security effectiveness at the checkpoint. So, that was a big improvement that we made right away.

Additionally, we increased the training for our TSA workforce, where we conducted more training that's instructor-led training, and led by instructors who are, typically, explosives experts. And so, we can show, for example, what we're seeing in the intelligence streams, and actually demonstrate to our officers what it is we're concerned about and what they should look at, not just for that particular piece of equipment, but what its variance might be, so they're alert for that as it might be going through the stream of commerce that goes through the checkpoints.

So, overall, we've made substantial improvements in our checkpoint operations. But, sir, to your point, the biggest improvement will be that technology infusion, which I think is right on the doorstep for us.

Senator NELSON. That red team test was done before you were the TSA Administrator?

Admiral PEKOSKE. Yes, sir.

Senator NELSON. Upon taking office, what did you say to your leadership team that you had to do to improve? Because the results of the surprise tests were appalling.

Admiral PEKOSKE. Yes, sir. The first thing we said is, we need to make immediate changes to be able to address these test results.

And second—and it was my opinion, as a passenger before I became the TSA Administrator—that we need to make a significant technology change at that checkpoint. And so, that was a—the two-pronged approach that—the training piece was already underway, we just enhanced that over the course of the fall. But, I think those three items will result in a significant improvement in our performance at the checkpoint.

Senator NELSON. Thank you.

Senator FISCHER. Thank you, Senator Nelson.

Senator Inhofe.

STATEMENT OF HON. JIM INHOFE,
U.S. SENATOR FROM OKLAHOMA

Senator INHOFE. Thank you, Madam Chair.

Admiral, numerous times last year, I and other members had gotten involved in this issue—the canines and what they're going to be doing, and the concern that we need to be using K9 teams. I think there is, kind of, unanimity on this Committee, when we had a hearing on this for air passenger and air cargo screening, and the current high demand for additional teams at the airport across the country.

Now, I don't know whether you were here or familiar with the hearing that we had when we had a witness, Steve Alterman. He's of the Cargo Airline Associations. And he said, quote, "I think one of the reasons that we do not yet have a K9 program is the lack of coordination between the various parts of TSA, and nobody seems to be totally in charge that can bang heads together and actually get it done." So, we're here to bang heads, this morning. What is your thought? Are you familiar with that statement that was made?

Admiral PEKOSKE. Yes, sir, I'm familiar. And I'm very, very familiar with the K9 program. I'm a huge fan of the K9 program. I think we need to expand it significantly from its current state. And literally, I look at the K9 program on a week-to-week basis. I'm totally focused on that.

Senator INHOFE. What seems to be the obstacle?

Admiral PEKOSKE. The obstacle is getting canines through our training program, down in San Antonio, which we have changed. We've changed the throughput of that training center from 300 canines per year to 350. And also, we're looking at sourcing our canines more domestically than internationally than we have in the past.

Senator INHOFE. Yes. Well, there's a lot of interest in that.

Admiral PEKOSKE. Yes, sir.

Senator INHOFE. Because we've talked about that before.

Mr. Kelly, I mentioned to you that I was going to bring this up, not expecting you'd necessarily have specific answers today, or thoughts today, that you may want to do it for the record. But, it's something that's of great concern to me. Now, China's state-owned rail business, the CRRC, is larger than all United States rails combined, and it benefits from the infinite subsidies. China's very good at that, once they get any competition. So, that's what we're faced with right now. In 2016, they sought to acquire Virtex. That's a United States railway. I sent a letter. I think some others did, too,

but, I remember, I sent a letter to Jack Liu—at that time, he was the Treasury Secretary—highlighting my concerns and asking the Committee on Foreign Investment in the United States—that's CFIUS—to review this transaction. Now, that happened in June of what year was that? Yes, 2016. And 6 months later, without any notice to us—now, keep in mind, the Department of Transportation, I don't believe, is one of the organizations that's on CFIUS. But, they didn't know anything that was going on that I was even aware of. Then, all of a sudden, they approved the sale—they approved the sale without any notification, and so forth.

Now, this has happened before. And I'm concerned about the way this process works. I would think that, certainly, the Members of the House and the Senate would like to have a voice in this and at least get a response before approving a sale. Are you into this issue? Is this something you're familiar with?

Mr. KELLY. Senator, I'm a little bit familiar with this issue, because your staff rose it—brought that to our attention of our staff. I did notice that there were a number of Senators that co-signed that letter; I think many of them here on this Committee. And I think the concerns that you've raised are significant concerns. However, I'm not sure that's—the role that the Department of Homeland Security has in this area. I will bring this up to our staff and try to get back to you on this.

Senator INHOFE. Yes.

Mr. KELLY. But, I question if this is the role of Homeland Security or if it's a bigger of a role for the Department of Treasury.

Senator INHOFE. Yes. And, you know, all due respect, I don't care whose role it is, but——

Mr. KELLY. Yes.

Senator INHOFE.—it's going to be something that's going to have to be addressed.

Now, you've refreshed my memory, and I do recall now, we had several people that were on this Committee that signed this letter with me. It was a letter from me. And it said that we have problems with this transaction. And, to my knowledge, it was done without any notification at all for any of the Members here. So, anything that you can do—there are several of us who are going to pursue a correction to this, or maybe a change in the way CFIUS works. But, I think it's important, particularly right now it's more significant, with what's happened in China in the recent years, than it was at that time. So, I just want to call that to the Committee's attention, and to yours, and anyone else out there who has an idea.

Thank you, Madam Chairman.

Senator FISCHER. Thank you, Senator Inhofe.

Senator Cortez Masto.

STATEMENT OF HON. CATHERINE CORTEZ MASTO, U.S. SENATOR FROM NEVADA

Senator CORTEZ MASTO. Thank you, Madam Chairwoman.

Mr. Kelly, you noted, in your testimony, the lack of key metrics to measure the success of the Transportation Worker Identification Credential Program's core objectives. And I'm a firm believer in data and metrics. And I'm wondering, in your opinion, are there

other TSA programs or spending that also struggle with these lack of proper performance metrics? And would you elaborate on that, a little bit, if you would.

Mr. KELLY. I think some of the questions concerning the covert testing is an area on the metrics on how well some of the screeners do in achieving the goals. That would be another area that I think there could be better metrics. If that answers your question.

Senator CORTEZ MASTO. Administrator, you agree?

Admiral PEKOSKE. I agree. We can do a lot better job with our metrics and really having outcome-focused metrics in place. With respect to the TSA workforce, we're making a significant number of changes in that regard, particularly the way we evaluate TSO performance. It had been a series of tests that were done over the course of the year, that, if a transportation security officer did not succeed in those tests, he or she was given a limited number of chances to pass it before they potentially lost their job. What we're doing now is, we're, over the course of the year, measuring their performance, so, at the end of the year, we can say, "Hey, this person has performed in an outstanding manner over the course of the year; so, therefore, they're recertified for their position." So, we've got a continuous stream of metrics and a lot less anxiety on the part of the workforce.

Senator CORTEZ MASTO. Thank you. And then, the last time we spoke, we also—and I appreciate you having a conversation with me—the concern about the budget for surface transportation and security. And I know you wanted time to get in there and take a look and figure out your priorities. And I heard a little bit today, but do you mind—I know you talked about Fiscal Year 2019 budget that you were involved with—can you talk a little bit more about your priorities, particularly as it pertains to what we're talking about for surface transportation?

Admiral PEKOSKE. Yes, ma'am. Appreciate the question.

And, you know, as I look at risk, I look at risk as being a combination of the threat, the vulnerability, and the consequence, should an attack occur in any particular mode of transportation. And I think we need to look at our risk quotient overall within the transportation system, and then allocate the resources where we see the greatest risk, currently, but also where risk might be developing in the future. And that's where the intelligence piece comes in mind, because I—I really don't want to see us in a position where we look at things in a static environment and say, "OK, the risk is here today," and we put resources—we allocate resources based on that, when the trending might be——

Senator CORTEZ MASTO. And so, can I just——

Admiral PEKOSKE. Right.

Senator CORTEZ MASTO. I'm sorry——

Admiral PEKOSKE. Sure.

Senator CORTEZ MASTO.—I only have 5 minutes.

Admiral PEKOSKE. Yes.

Senator CORTEZ MASTO. So, does that mean you're looking at that now to determine staffing needs——

Admiral PEKOSKE. Yes, ma'am.

Senator CORTEZ MASTO.—resource needs for technology, resource needs that you will need, particularly in this budget area, for surface transportation?

Admiral PEKOSKE. Yes, ma'am.

Senator Cortez Masto: Is that correct?

Admiral PEKOSKE. Yes, ma'am.

Senator CORTEZ MASTO. Can you talk a little bit about new technologies? For—and let me just put this in perspective. We have seen, from smart buildings to smart technology in our transportation sector—and, particularly in Nevada, this is really exciting area for us and across the country. I'm wondering if you can talk a little bit about these new technologies that show promise for safety and security, that you underscored in your testimony, when it comes to smart transportation technology?

Admiral PEKOSKE. Yes, ma'am. The one that I highlighted in my testimony and in my oral statement was the standoff detection equipment that allows us to see if a person might be—might have a—an IED on their body. And what this does is, it doesn't transmit any energy toward the individual whatsoever, it just reads the energy that somebody's body is transmitting. And I took a demonstration of it a couple of weeks ago. It's very, very good. And this is one of the things that TSA does well, I think, is, we look at technology that's out there, in combination with the Department of Homeland Security science and technology directorate, and we do testing for the industry, and we complete testing and then give them a list of manufacturers whose results conform to what our standards are. And then they can go buy it off of our list of certified equipment, if you will. So, that's a very promising area of work for us.

Senator CORTEZ MASTO. And is this something you're also looking at to incorporate into your budget, this new technology that you think might be helpful with security?

Admiral PEKOSKE. What we incorporate into our budget, Senator, there is really the testing of the technology, not the purchase——

Senator CORTEZ MASTO. OK.

Admiral PEKOSKE.—of the technology.

Senator CORTEZ MASTO. OK.

Admiral PEKOSKE. Right.

Senator CORTEZ MASTO. Appreciate that.

Admiral PEKOSKE. Right.

Senator CORTEZ MASTO. Thank you.

Admiral PEKOSKE. But, I look—be looking for technology overall, anything that might apply in aviation certainly into surface would be a bonus, as well.

Senator CORTEZ MASTO. I appreciate that.

Thank you both.

Senator FISCHER. Thank you, Senator Cortez Masto.

Senator Hassan.

STATEMENT OF HON. MAGGIE HASSAN,
U.S. SENATOR FROM NEW HAMPSHIRE

Senator HASSAN. Well, thank you, Senator Fischer and Senator Peters.

And welcome, to our witnesses, this afternoon.

Administrator Pekoske, I wanted to start with you. One challenge we faced in New Hampshire is the need to ensure that our first responders in the Granite State have enough information about what dangerous chemicals or other products are traveling through by freight rail. Back in 2013, there was an awful derailment and explosion in Lac-Megantic, Quebec, which is just over the border from New Hampshire, in Canada, killing over 40 people and—after a huge fire, petroleum and petroleum byproducts polluting an entire town. So, first responders need this information in order to adequately respond if a derailment or terrorist attack were to happen. And we have seen some improvement in sharing information over recent years, but I'd like to hear your thoughts on how Federal, State, and local entities can continue to collaborate with industry to share information and best practices so that local first responders aren't caught off-guard when a security incident occurs.

Admiral PEKOSKE. Yes, ma'am. I think it's very important that everybody, like you said, collaborates on this, because the first responders, maybe at the State level, the local level——

Senator HASSAN. Yes.

Admiral PEKOSKE.—they may be at the Federal level—if they're at the Federal level, they may be from multiple Federal agencies.

Senator HASSAN. Right.

Admiral PEKOSKE. And we do a process called the ISTEP, Intermodal Security Exercise Training Program. And part of it is training. But, where training really becomes embedded is in exercises, as well. And so, as we run exercises, we can see where there might be some shortcomings across the spectrum of first responders, and be able to bridge that.

Senator HASSAN. Well, I would appreciate—you know, I'd look forward to talking with you more about it, because it became—I think, for all states, it's a real issue. Sometimes, the owners of the railroads or their customers don't want to share specific information because it's proprietary. And we need to figure out a way to make sure they do that and we all understand the limits of the information-sharing.

To both of you, TSA has also coordinated with the Department of Transportation to assess critical infrastructure, such as tunnels and bridges. As of September 2015, TSA reported it had provided remediation recommendations to 81 of 100 high-risk bridges. Our crumbling infrastructure poses a really significant and serious security threat. That's one of the reasons my senior Senator, Senator Shaheen, and I introduced the Safe Bridges Act, which would provide much needed funding for repairing and replacing bridges categorized as structurally deficient. So, how important is infrastructure investment to our Nation's security? And we'll start with you, Administrator, and then Mr. Kelly. Either one of you——

Admiral PEKOSKE. Sure. I think infrastructure investment's critical to security, because—I mean, I think we should look at infrastructure investment as a way to build in security into that infrastructure as we're renewing it. It's a significant effort on our part, with respect to airports, and certainly with surface transportation systems. And, you know, the earlier we can have a dialogue with owners and operators of systems that are considering an infrastructure investment, the more we can put our design desires into the

build of that infrastructure. And that gets to good pricing and good project management.

Senator HASSAN. Thank you.

Mr. Kelly.

Mr. KELLY. I agree with the Administrator. If you have a crumbling infrastructure, it's much easier to break those——

Senator HASSAN. Yes.

Mr. KELLY.—than it is to have the infrastructure that's designed to actually withstand some things. Just look at the way the building codes in San Francisco has enhanced the buildings to deal with earthquakes.

Senator HASSAN. Sure. Well, thank you for that.

I want to go back, for a minute, on the issue of our rail system and our security. To Administrator Pekoske, I—as I understand it, TSA is working to employ—and you guys have been talking about it—a risk-based approach to securing the passenger rail system. Part of that risk-based approach is to assess whether the intelligence points to the likelihood or probability that terrorist actors would select passenger rail systems as a target. The other part of risk-based approach is understanding passenger rail's vulnerability to an attack and working to mitigate the effects of a successful attack. While intelligence may not indicate the likelihood of an attack, intelligence isn't foolproof, right? We all know that. So, what measures are currently in place that would seek to prevent a terrorist attack on passenger rail as a contingency plan in the event that our intelligence underestimates the likelihood of attack?

Admiral PEKOSKE. Senator, I think, you know, a good part of that is look—is doing vulnerability assessments and figuring out where you might make some enhancements to your security. And we have a program that's called BASE. It stands for Baseline Assessment for Security Enhancement. So, essentially, we look at a system and say, "Hey, here's where it is from a security perspective. Here's where we can enhance it. And, on the margin, what's our greatest return per enhancement so that the investment goes the furthest?"

Senator HASSAN. Well, thank you. And seeing my time is up, Mr. Kelly, I will follow up with you more about some of the progress or delays on the crosscutting, risk-based approach that the Department is supposed to be undertaking.

Mr. KELLY. OK.

Senator HASSAN. Thank you.

Senator FISCHER. Thank you, Senator Hassan.

Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR, U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much, Madam Chairman. And thank you, to you, as well, Senator Peters, this important hearing.

And, in Minnesota, we host a lot of big events, including the Super Bowl, which is coming up. Just wanted to do a little advertisement there, even though, sadly, our team won't be in it. But, we will be hosting a million people in less than 2 weeks. So, league officials have said that it's going to be one—the most transpor-

tation-centric event in NFL history. You're nodding your head, Mr. Pekoske. What steps are you taking to efficiently screen people at the airport and people at the game? And I know you can't go into all the details, but I would assume that this is—a general answer would apply to all events that you do.

Admiral PEKOSKE. Yes, Senator. It's—we're doing an awful lot with respect to Super Bowl, as you might imagine. First off, on the airport side, we work very closely with the airports and the airlines to figure out when the bulk of passengers will be arriving—actually which flights at which times—so that we can put the right resources in place to be able to handle them as they come into the airport and certainly as they depart the airport once the game is over. This is, as you said, a very transportation-centric Super Bowl. Some of our Viper Teams will be present in Minneapolis for that, assisting State and local, and coordinating very carefully with them.

And, of course, with respect to screening, we have expertise in screening, and provide that expertise to the stadium owners and operators.

Senator KLOBUCHAR. Very good. And I've always been a big fan of the Viper units, and including the K9 units. As you know, we had some issues at the airport, a while back, due to a number of factors. And it was the K9 units that came in. I maybe have told you that two dogs were flown in from Maui, so they came to Minnesota from Maui; kind of wrecked their life, but that's OK. They seem happy now. And so, around 50 percent of the guests at the Super Bowl are going to arrive on the metro transit's lite rail. Could you talk about how the Viper Teams will help secure the metro transit train stations that'll be used to get guests to and from the game?

Admiral PEKOSKE. Well, Viper Teams, Senator, are married up with K9s, so that provides a very good force multiplier for the Viper Teams. Additionally, the Viper Teams provide that visible presence so that people see that, they get—you know, comforted by the fact that there is a security presence there. But, key to the Viper Team's success is the good coordination they have with State and local officials. And part of this process is to talk a lot, and coordinate a lot before the event occurs.

Senator KLOBUCHAR. During your confirmation hearing last year, I asked you about the greatest challenges TSA faces. In response, you stated that "workforce training and developing and deploying new technology were at the top of your list." Where does TSA stand with its workforce training now? What things have you done?

Admiral PEKOSKE. We place an awful lot of emphasis on the workforce, period, and workforce training, in particular. And we've got in place now, as we're—we're beginning to roll out a new career progression for our transportation security officer workforce, which essentially lays out for that work force, which is the bulk of the Transportation Security Administration, what a progression would be from an entry-level transportation security officer to a transportation security manager, the most senior person at the checkpoint. And along the way, we provide required in-person and onsite training, in addition to pay increases, once the training is achieved and certifications are acquired. So, the whole idea was to really map

out for our workforce what a career in TSA, and what a career progression would look like, and what kind of training that we were committing, as an organization, to provide to them.

Senator KLOBUCHAR. Very good.

The freight rail system, one question on this, with over 4,400 route miles, 20 railroad companies are critical to efficient movement of goods. We have a lot coming through, as you can imagine, being next to North Dakota, where the oil is. We've got biofuels coming through. We've got things coming through Canada. And I think people would be surprised at how much rail we have in Minnesota. According to your testimony, TSA will be hosting this Surface Public Area Security Summit next month to discuss best practices, to—collaboration with the industry. Could you talk about the security of freight rail?

Admiral PEKOSKE. We've invited freight rail to attend, and I expect that we'll have a good representation from freight rail. And we'll have a good representation from across the board, including a good number of people from the aviation sector. So, it's a really great opportunity to spend a day, talk about overall public-area security, and move it forward, getting best practices from the different modes of transportation.

Senator KLOBUCHAR. All right. Thank you very much.

Senator FISCHER. Thank you, Senator Klobuchar.

Senator Cantwell.

STATEMENT OF HON. MARIA CANTWELL,
U.S. SENATOR FROM WASHINGTON

Senator CANTWELL. Thank you, Madam Chair. And thank the witnesses. And thank you to Ranking Member Peters for holding this hearing.

All of these issues are so important. And I think you've heard from many members: dogs, dogs, dogs. Because we know the effectiveness of the K9 units. And we're using them even at our ports as it relates to our ferry transportation system. And I'm sure people are using them on security for other aspects of rail and other things.

But, I have a letter from the Sea-Tac folks, because you know that Sea-Tac is one of our fastest-growing airports in the United States. And I quote from it. And they say they deeply value the good relationship with TSA and believe that their solutions continue to require some engagement from top TSA leadership. I would assume they mean you. So, their issue, which we have seen, is, when we have the K9 units that we need, the airport functions well. When we don't have the K9 units, it struggles to really reach capacity.

Admiral PEKOSKE. Right.

Senator CANTWELL. So, we've had some TSA staffing reductions because of those checkpoint issues, given, you know, the new technology that's being implemented. But, we're down from ten—nine K9 units, ten that were allocated, to five. And this growth that we are seeing is just phenomenal. So, I wondered if I could get your comments on how you could help us with that?

Admiral PEKOSKE. Yes, ma'am. You should have all of your K9 teams back in full force by the end of March. So, that's good news.

And that's part of our effort to try to increase the throughput through our training center, and really very carefully monitoring the allocation of K9 resources across the board. As you and I have discussed, you know, as you know, we have 372 passenger screening K9 teams authorized in the TSA budget. I think that number needs to go up, and up substantially. And so, I—you know, I would like to see that go up over the course of successive years so we get much more capacity, because canines are so critical to security effectiveness, for sure, and also to helping us manage throughput issues at the airport.

Senator CANTWELL. And does that include the training partnership program language, as well?

Admiral PEKOSKE. The——

Senator CANTWELL. Ability to do training verification by third parties.

Admiral PEKOSKE. Yes, ma'am. In fact, we have a——

Senator CANTWELL. I mean, to reach that number, do we need to do both of those things?

Admiral PEKOSKE. I think to reach the number—I think we can reach the number with the current training center that we have, the initial step up, in a couple of years. But, the third-party process is moving along pretty vigorously. And we have an industry day scheduled for a week from today, actually. And I'm very optimistic about that third-party K9 program. It's got my attention, as do K9s overall. And I would expect that we'll be able to launch that program in the next couple of months, once we get——

Senator CANTWELL. And what about the——

Admiral PEKOSKE.—once we get industry——

Senator CANTWELL. And what about the staffing levels of TSA? Could you look at that for me, please, and give me comments at Sea-Tac?

Admiral PEKOSKE. Yes, ma'am.

Senator CANTWELL. Thank you.

Well, Mr. Chairman—I mean, Madam Chairman, I definitely think that we need to take today's hearing as an opportunity to work with TSA on increasing those K9 units. They do such fabulous work. And it is just an amazing level of deterrence that we need to have everywhere. And so, look forward to working with the Chairman and everybody on how we get that over the goal line.

Thank you.

Senator FISCHER. Thank you, Senator.

We've been joined by the Chair of the Committee, Senator Thune.

STATEMENT OF HON. JOHN THUNE,
U.S. SENATOR FROM SOUTH DAKOTA

The CHAIRMAN. Thank you, Chairman Fischer, for holding today's hearing.

And thanks, to Admiral Pekoske and to Mr. Kelly, for being here.

Admiral, I would also like to recognize the hard work of your TSA officers. Like most people here, I travel between South Dakota and Washington, D.C., weekly, and I always appreciate the professionalism and the diligence of your TSA teams. So, please thank them for all that they do in keeping us safe.

And I also want to just say a quick word about both the Surface and Maritime Transportation Security Act and the TSA Modernization Act that this Committee has approved on a bipartisan basis. Both bills seek to strengthen our transportation security, guarding against terrorist threats to our infrastructure and the traveling public by modernizing the way TSA is organized and ensuring that resources are allocated through a risk-based strategy. I remain committed to these important pieces of legislation. I'm hopeful that the full Senate will consider them, sooner rather than later.

Admiral, let me just ask you. You've been in the position now for 5 months. Can you describe what you see as your biggest challenge in the surface security area?

Admiral PEKOSKE. Sir, thank you. And thank you for the comments about the TSA workforce. It's greatly appreciated. And I know a number of the transportation security officers and other staff in TSA watch this hearing, and they really genuinely appreciate your comments and the comments of the rest of the Committee members on their performance.

In terms of challenges overall, I think the—one of the biggest challenges we face is getting more technology into the organization. And it goes across the board, whether it's aviation or surface. And the other challenge is—and you'll see in the strategy, that I have in draft form right now—that I would like to bring to all the members of the Committee in draft form to get your feedback on—but, one of the key tenets of that strategy is to lead transportation security, emphasis on "lead." And the second is to accelerate action on the part of TSA. And that's been a theme I've seen since I've been in the position for 5 months. And certainly I've heard from our industry stakeholders, from Members of Congress, both on the authorization and the appropriations side, is, we just need to get, as a business that we're about, in a much quicker way, get the decisions faster and get the solutions faster so that we can get more K9 teams deployed quicker, that we can get more CT technology at the checkpoint quicker, that we can test more technology for surface transportation quicker than what we do today.

The CHAIRMAN. Yes.

Mr. Kelly, thank you for your testimony updating us on TSA's actions to address your recommendations. I understand that some progress has been made, but there are still some actions that need to be completed.

Mr. KELLY. That is correct, Senator.

The CHAIRMAN. I also am pleased to hear that you think that our bill, the Surface and Maritime Transportation Security Act, addresses many of the remaining issues. Going forward, what do you believe TSA's top priority should be for improving surface security?

Mr. KELLY. For surface security, I believe that they need to focus on a risk-based strategy for all of—all surfaces. That will likely reallocate additional money toward surface-based transportation, and that will provide greater resources and oversights in those areas, which should improve security on surface transportation.

The CHAIRMAN. Admiral, we've heard, in the past, complaints from stakeholders of redundant checks, and from multiple Federal agencies. What is TSA doing to coordinate with other Federal, State, and local agencies to ensure the proper level of security is

in place, but, at the same time, prevent overly burdensome and repeated inspections by multiple government agencies?

Admiral PEKOSKE. Mr. Chairman, you know, one of our key areas of focuses is the passenger experience and our relationships with industry. And, you know, I'd be interested in any examples that any partner has where they might see some duplication between what TSA does and what another agency does. Additionally, it's incumbent upon me to coordinate, without even any of that information, with my other partners, certainly in the Federal Government, to make sure that we eliminate or reduce as much as possible any redundancies between our efforts. Because it's just not efficient, and it's really not good for our stakeholders to see things coming from multiple different directions. We ought to be able to coordinate that better.

The CHAIRMAN. OK.

Madam Chair, thank you.

Senator FISCHER. Thank you, Senator Thune.

I would like to thank the panelists for being here today. Administrator, Mr. Kelly, we appreciate the information that you've provided to us.

The hearing record will remain open for 2 weeks. And, during this time, Senators are asked to submit any questions for the record. Upon receipt, the witnesses are requested to submit their written answers to the Committee as soon as possible.

Again, thank you, gentlemen.

The hearing is adjourned.

[Whereupon, at 3:40 p.m., the hearing was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO HON. DAVID P. PEKOSKE

Question 1. Amid public calls by Al Qaeda and other terrorist groups to target our rail systems, what more can be done to better secure our passenger and freight rail infrastructure?

Answer. The Transportation Security Administration (TSA) addresses the risks to freight and passenger railroads through information sharing, including classified information (ensuring that railroad security officials are aware of threats), planning (preparing plans for countermeasures that can be employed when the level of threat is elevated), training (providing training for employees to enhance their awareness and understanding), and exercises (providing venues and opportunities to test plans and operational practices in order to be better prepared). TSA evaluates technology on behalf of industry to provide products to help identify and or mitigate threat on passenger and freight rail systems.

For over 12 years TSA has partnered with passenger and freight rail industry stakeholders to establish ongoing testbeds that provide critical data and information that stakeholders can use to improve their infrastructure protection. These testbeds assess both marketplace and emerging technology, integrated into sophisticated, layered systems; thereby expanding and encouraging the technology marketplace while providing industry with proven solutions and concepts of operation that they can adapt to their particular needs. Examples of these testbeds include a comprehensive intrusion detection and protection testbed in the Northern New Jersey/Newark area and advanced technology at the Tennessee River and Plattsmouth railroad bridges.

In response to Al Qaeda in the Arabian Peninsula's (AQAP) Inspire 17 magazine published in August 2017, which gave detailed instructions on how to build and deploy a train derail device and encouraged would-be jihadists to use it:

- TSA convened a meeting of subject matter experts from the Federal Bureau of Investigation (FBI) and the Federal Railroad Administration (FRA) to ascertain the possible consequences associated with the use of this device. TSA and the FBI determined it would be beneficial to construct and test the Inspire derail device.
- TSA's Office of Requirements and Capabilities Analysis conducted tests of the improvised derail device at the Transportation Technology Test Center in Pueblo, CO in December 2017, with representatives from the FBI, FRA, and the National Transportation Safety Board in attendance to observe the tests. The full results of the tests are Sensitive Security Information and can be provided upon request.

Question 2. Given recent incidents of terrorists targeting public spaces, what is TSA doing and what more can be done to protect those transportation open spaces?

Answer. The Transportation Security Administration (TSA) partners closely with stakeholders in all modes of transportation to discuss and develop best practices to enhance security in public areas. In September 2016, TSA began hosting Public Area Security Summits with industry, government, academic, and international stakeholders to devise a strategy for information sharing, and protecting infrastructure from emerging threats to public spaces of transportation venues. Participation of both government and industry executives provides a unique opportunity to leverage expertise and resources, and collaborate on security plans moving forward. This program also enables strategic alignment and unity of effort across numerous entities within the public spaces. The work of the group resulted in the publication of a Public Area Security National Framework in May 2017, with 11 corresponding recommendations. Additionally, the group continues to meet—most recently in early February 2018—to discuss the implementation of the recommendations and share best practices and lessons learned. The Public Area Security Summits will continue bi-annually, with the next meeting scheduled for fall 2018.

Various airports have adopted many of the recommendations and the continued meetings provide a forum to share best practices. For example, in 2017 MASSPORT hosted an Aviation Security Meta-Leadership Symposium for their employees as well as local stakeholders for threat awareness education as a direct result of the public area security summits and framework.

The Framework recommendations included: Cultivate Relationships; Develop Communication Strategies to Enhance Information Exchanges; Enhance Situational Awareness; Expand Threat Awareness Education; Develop Joint Risk Frameworks & Enhance Joint Vulnerability Assessments; Establish Airport Operations Centers; Conduct Background Checks & Threat Assessments of Public Area Workers; Conduct Workforce Employee Training; Develop, Conduct, and Practice Exercises & Response Drills; Invest in Innovative Construction Designs; and Coordinate Response Planning.

Question 3. As a former Vice Commandant of the Coast Guard, I know you are familiar with the Coast Guard's roles and missions, can you discuss what steps you are taking to ensure there are no seams that terrorists can exploit between where the Coast Guard's maritime and TSA's transportation responsibilities meet?

Answer. The Transportation Security Administration (TSA) supports the U.S. Coast Guard (USCG) in the maritime mode, as the USCG is the lead Federal agency for maritime security. TSA leverages its expertise in passenger screening, explosives detection, transportation worker credentialing, and multi-modal security to support the USCG in coordinating and conducting interagency security efforts for the maritime mode. As the USCG is the lead Federal agency for maritime security, TSA supports the USCG in its maritime security efforts and in coordinating interagency efforts for the maritime mode. TSA works closely with the USCG, as well as other government agency maritime partners, to provide subject matter expertise to Federal working groups, disseminate security information to the public, and review interagency documents. TSA supports the USCG by providing TSA-developed maritime security training materials and coordinating maritime security exercises with maritime stakeholders to strengthen security plans, policies and procedures. TSA also works closely with USCG HQ offices in support of their cybersecurity efforts, providing information on cybersecurity measures and resources to the maritime industry.

Question 4. Administrator Pekoske, I am aware of several overdue letters of response and reports that TSA owes to this Committee; including five overdue reports required by the FAA Extension, Safety, and Security Act of 2016, two from the Homeland Security Act of 2002, as amended by section 3 of the Transportation Security Acquisition Reform Act, and the 2017 Annual Report on Transportation Security.

a. Has TSA sent these reports to DHS for clearance?

b. When can we expect to see these reports?

Answer. The Transportation Security Administration (TSA) currently does not have any outstanding overdue reports to the Senate Committee on Commerce, Science and Transportation. In 2017, TSA submitted to the Committee the reports required by the FAA Extension, Safety, and Security Act of 2016, the Homeland Security Act of 2002, as amended by section 3 of the Transportation Security Acquisition Reform Act, and the 2017 Annual Report on Transportation Security. Included in those submissions were the following eight reports:

1. Implementation of the Rap Back Service for Recurrent Vetting of TSA-Regulated Populations on April 5, 2017
2. TSA Report on the Insider Threat to Aviation on May 4, 2017
3. TSA Office of Global Strategies Comprehensive Workforce Assessment on May 25, 2017
4. TSA Security Coordination Enhancement Plan on June 28, 2017
5. TSA Pre✓® Application Program Fee Revenue and Investments on September 29, 2017
6. Small Business Contracting Goals Report on April 7, 2017
7. Strategic Five-Year Technology Investment Plan Biennial Refresh on December 19, 2017
8. 2017 Annual Report on Transportation Security on December 20, 2017

TSA remains committed to ensuring the timely submission of all required letters and reports.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DEB FISCHER TO HON. DAVID P. PEKOSKE

Question 1. Administrator Pekoske, can you give the Committee an update on TSA's efforts to review and reform the TWIC program as a result of the agency's comprehensive risk analysis?

Answer. The Transportation Worker Identification Credential (TWIC)® program is a jointly managed program between the Transportation Security Administration (TSA) for the security threat assessment and card issuance and the United States Coast Guard for the use and access at regulated maritime ports and facilities. In 2017, the TSA commissioned the Homeland Security Operational Analysis Center (HSOAC), a federally funded research and development center operated by the RAND Corporation, to conduct an independent review of its Security Threat Assessment (STA) controls and risks. The review found that while TWIC® controls are in line with Federal best practices and standards, possible improvements were identified for each phase of the TSA STA process. Where controls were less developed, HSOAC, provided recommendations on new controls or areas where controls could be strengthened for ensuring the security of the TWIC® program. TSA is using the recommendations from this review to develop a control and quality management plan to augment its risk management processes. By improving its framework for actively identifying and managing controls and risk tolerances, the TSA TWIC® program will minimize security vulnerabilities to the STA process and provide reasonable assurance that the program achieves its security objectives. TSA will brief the Committee on the enhancements to its risk management process after it has implemented the management plan, including an internal control framework and enhanced adjudication and security controls for conducting STAs. TSA plans to complete implementation in by the end of calendar year 2018.

Question 2. Administrator Pekoske, during a Surface Transportation and Merchant Marine Infrastructure, Safety, and Security Subcommittee hearing in 2016 we heard testimony that TSA has much to learn in the cybersecurity realm. What actions have you taken, or plan to take, to improve TSA's cybersecurity posture?

Answer. In accordance with all the cybersecurity Executive Orders, Binding Operational Directives, and Policy Memos the Transportation Security Administration (TSA) has continued to evolve its cybersecurity posture, personnel, and capabilities. TSA is mitigating the cybersecurity risks to TSA's data, systems, and networks through the implementation of tools that: monitor privileged user activity; detect malicious content in web traffic and e-mails; and accelerate the detection of Indicators of Compromise (IOC). In 2017 TSA awarded three strategic cybersecurity contracts. These contracts have enabled TSA to augment its cybersecurity workforces in the areas of: Monitoring and Cybersecurity Network Defense; Security Infrastructure and Vulnerability Assessments; Digital Forensics; and Cybersecurity Governance Risk Compliance.

For Surface Transportation Systems, TSA's Office of Security Policy and Industry Engagement (OSPIE) works in coordination with TSA's Offices of Intelligence and Analysis, Information Technology, Security Operations, and with the other Sector Specific Agencies (SSA), Department of Transportation and the U.S. Coast Guard with the objective of awareness and outreach. Support for the Sector's cyber risk management efforts is done through a non-operational approach centered on education, facilitation, and information sharing. The purpose of these efforts are to develop, deploy, and promote Sector-focused cybersecurity initiatives, programs, tools, strategies, and threat and intelligence information sharing products that support the implementation of national mandates, strategies, policies, directives, and priorities.

Current Initiatives:

- Facilitate collaboration between industry and government partners to promote cybersecurity risk management programs and resources with the goals of:
  - Supporting the increased use of existing government resources.
  - Increasing the industries' operational resilience and ability to manage cyber risk.
    - Regional Surface Transportation Cybersecurity Workshops—Partner with the DHS Office of Cybersecurity & Communications and TSA Regional Surface Inspectors to deliver facilitated workshops highlighting the many DHS and Federal cyber-risk management resources that are available to critical infrastructure partners.

- We continue to practice an approach of continuous improvement based on feedback received during our workshops and hot-wash sessions.
- As a result, industry stakeholders were added as speakers at the last two workshops to share a recent incident they have experienced and/or their cybersecurity risk management strategy. We also added in-depth discussion and Q&A about their take-aways from their workshop participation.
- On December 13, 2017, one workshop took place in Cleveland, OH. There are five more workshops planned for Fiscal Year (FY) 2018:
  - Atlanta, GA on March 14, 2018
  - Washington, DC on March 21, 2018
  - Dallas, TX in late April/May 2018
  - Los Angeles, CA in late June/July 2018
  - Pacific Northwest in late July/August 2018
- Past participants have included stakeholders from Surface, Aviation and Maritime modes.

◦ Distribute Cyber Security Awareness guides and the Surface Transportation Cybersecurity Toolkit.

◦ Sponsor and participate as a member on the American Public Transportation Association (APTA), Enterprise Cybersecurity Working Group (ECSWG), and Control and Communications Systems Working Group (CCSWG) Recommended Practice Working Groups. Current projects include:

◦ Guidance document for a transit agency's CIO, CISO, and HR to use to gain buy-in from their Management, C-Suite and/or Board of Directors that:
- Provides rationale for creating an active cybersecurity awareness program.
- A call to action that cybersecurity is everyone's job.

◦ Update to Recommended Practice Part 2 (2013)—"Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones" to align to the Framework.

◦ Rail Car Cybersecurity White Paper.

◦ Transit Bus Cybersecurity White Paper.

◦ Revising the TSA Pipeline Cybersecurity Guidelines (2011) to align with the NIST Cyber Security Framework and we expect to release in 2018.

◦ Developing cybersecurity incident reporting guidelines for Mass Transit and Freight Rail operators that both align with existing regulations and support more robust Federal incident response processes.

◦ Expand partnerships and coordination efforts with our DOT/NHTSA and industry stakeholders on vehicle cybersecurity issues.

Recent Accomplishments:

- Planned and facilitated a series of four regional Cybersecurity Workshops in FY 2017. The workshops provided a baseline awareness of existing U.S. Government cybersecurity support programs and allowed stakeholders to share best practices and lessons learned with one another. Additionally, the facilitated discussion component served as an opportunity for participants to both discuss industry's cybersecurity challenges and for them to share their organization's best practices.

  ◦ FY 2017 Workshop locations:
  - Arlington, VA (DC Metro Area), co-hosted by Arlington County—ART
  - Pittsburgh, PA, co-hosted by Port Authority of Allegheny County
  - St. Louis, MO, co-hosted by Bi-State Development Agency/Metro Transit
  - Oakland, CA (San Francisco Bay Area), co-hosted by Bay Area Rapid Transit
- Finalized and distributed over 56,000 thousand cybersecurity-specific awareness guides.
- Developed, promoted, and disseminated the Surface Transportation Cybersecurity Resource Toolkit for Small & Midsize Business (SMB) that provides guid-

ance on how to incorporate cyber risk into an organization's existing risk management and governance process.

- Developed and disseminated Cybersecurity Awareness Messages (CAMs) and Surface Information Bulletins that covered:
  - Cyber Petya Ransomware Attacks.
  - Observance of 13th National Cybersecurity Awareness Month.
  - Ransomware Attack Awareness: how to protect & how to respond.
- Collaborated with industry partners to provide cybersecurity focused support at various industry sponsored modal meetings, workshops, and conferences.
- Participated as a member and collaborated on various internal and joint public/private TSS cybersecurity working groups that included:
  - Transportation Systems Sector Cyber Working Group (TSSCWG).

Bi-weekly TSA Cyber Coordination working group.

Question 3. Administrator Pekoske, I understand TSA is testing a system that could detect concealed explosives and suicide vests in crowded areas like public transit systems.

Question 3a. Could you provide background and an update on this program?

Answer. TSA has been actively exploring ways to detect threats on persons within the public transportation environment for a number of years. Recent advances in technology have dramatically improved performance while reducing system cost. TSA continuously assesses the technology marketplace and collaborates with technology providers to improve their products. Technology involving standoff detection of concealed threats is always of significant interest.

TSA has worked with several leading standoff detection technologies since the first prototypes appeared around 2005. Two leading vendors' units should be available for sale to the security industry by early to mid-summer of 2018.

Question 3b. What is the program's detection rate?

Answer. Both systems have shown extremely high rates of detection against a wide range of explosive threats, with very low rates of false positives. While precise detection rates are classified, upon request TSA can provide a briefing in an appropriate venue.

Question 3c. Would adoption of this technology slow the movement of people going into or out of a public transit system?

Answer. No. The two standoff detection technologies being assessed operate in real time, generally requiring only about one second of visibility to detect. Under many circumstances, they can also screen several persons at the same time. TSA surface security technologies are focused on the ability to detect threats without impeding the free movement of people through the venue.

Question 4. Administrator Pekoske, as part of its surface transportation security portfolio, TSA does work to identify and issue recommendations to the pipeline industry related to system security. For example, in 2016, TSA completed a review, required by the 9/11 Commission Act, to review the security of the Nation's top 100 pipeline systems. Do you have any updates on TSA's work to detect threats and provide support for pipeline security? Additionally, TSA has a memorandum of understanding with the Pipeline and Hazardous Materials Safety Administration (PHMSA) to cooperate on pipeline security threats. Have you worked to develop a relationship with PHMSA and Administrator Skip Elliott to support PHMSA's work on pipeline security?

Answer. The Transportation Security Administration (TSA) continues to work collaboratively with the pipeline industry to identify threats and provide support for pipeline security.

Some of these TSA initiatives include:

- Regular pipeline threat assessments and briefings administered by TSA's Office of Intelligence and Analysis (OIA). Threat updates are provided, at a minimum during monthly stakeholder conference calls and annually to over 100 industry security representatives at the International Pipeline Security Forum.
- Issuing Pipeline Security Guidelines (dated 2011) for enhancing physical and cybersecurity. TSA worked with industry stakeholders to update these Guidelines specifically with regard to cybersecurity and we expect to release in 2018.
- TSA Evaluates corporate security policies and procedures of the Nation's top 100 pipeline systems and provides recommendations for a more robust corporate security program.

- The TSA Critical Facility Security Review (CFSR) program focuses on the collection of site-specific facility information, and provides recommendations for improving the security posture of critical pipeline facilities. In FY2017, TSA conducted 70 CFSRs.
- TSA maintains ongoing security technology testbeds at two major pipeline sites, in partnership with a major U.S. pipeline company.
- The TSA Intermodal Security Training and Exercise program provides exercise, training, and security planning tools in a variety of formats (table top exercises, full scale exercise, workshops).
- TSA distributed over 10,800 Pipeline Counterterrorism Guides in FY2017 to pipeline owners/operators as a means to enhance security awareness and employee vigilance.
- TSA uses multiple platforms to share timely and relevant information including monthly stakeholder calls, security and incident awareness messaging, collaboration with industry trade associations, and active involvement with industry's Oil and Natural Gas Sector Coordinating Council and their initiatives.

Indicative of TSA's active and longstanding partnership with PHMSA on pipeline safety and security matters, TSA's Surface Division Director recently met with PHMSA Administrator Skip Elliott. TSA and PHMSA have a memorandum of understanding detailing the various ways the agencies cooperate on matters relating to pipeline security.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BILL NELSON TO HON. DAVID P. PEKOSKE

Reimbursements to Airports. Following the September 11th terrorist attacks, several airports across the country, including many in Florida, installed in-line baggage screening systems with the understanding that they would be reimbursed by the TSA. My understanding is that these airports are owed at least 217 million dollars.

Question 1. When can we expect the TSA to begin the process for reimbursing these airports?

Answer. In November 2017, the Transportation Security Administration (TSA) completed the seven-step process, and finalized the Airport Reimbursement List, as outlined in the TSA Reimbursement Review and Validation Plan for In-Line Baggage Screening Systems, Fiscal Year (FY) 2016 Report to Congress (June 16, 2016). The list identifies 16 projects across 14 airports eligible for funding totaling $217,879,014.36. With the passage of the Fiscal Year 2018 Consolidated Appropriations Act, (Public Law 115–141), $50 million was made available to begin satisfying these claims. TSA intends to implement a pro rata distribution of the funds allocated toward reimbursement. This allocation process was determined by TSA to be an objective, transparent and equitable distribution of the discretionary appropriations made available for the purpose of reimbursing airports for eligible projects. Under the pro rata allocation method, each airport is equally entitled to a share of their eligible costs on a pro rata basis.

Using this methodology, an individual airport's reimbursement will be based on the airport's eligible reimbursable amount as a percentage of the total eligible amount for all airports. This percentage will then be applied against the total amount of funding available to determine the amount that will be reimbursed to a specific airport. The distribution of the $50 million will be implemented in FY 2018.

Funding For Surface Security. We see the very real threats to our surface security systems, yet less than two percent of the TSA's budget is devoted to surface transportation. And more problematically, the administration has proposed cuts to grant programs and VIPER teams that support surface transportation security.

Question 2. Given the recent and continued incidents, shouldn't we reexamine the amount of funding for surface security systems?

Answer. The primary responsibility for security in surface transportation lies with the owners and operators of those systems and companies, because the components of the transportation network are largely privately owned and operated. Consistent with its authorities and responsibility for transportation security, the Transportation Security Administration (TSA) supports security of surface transportation by developing policies and resources, as well as working with system owners/operators in identifying, developing, and implementing remediation strategies to include unpredictable operational deterrence, preparedness and response exercises, improving critical infrastructure resilience, front line employee security training, and public awareness campaigns and materials.

Combined total funding for surface transportation security is much greater than reflected in the TSA budget. Operators and local/regional authorities commit funding to security and the Department of Homeland Security is appropriated funding for surface transportation security grant programs, which has totaled over $2.5 billion since Fiscal Year 2006.

Although TSA's budget for surface transportation is small compared to the aviation sector, the Nation realizes a significant return from this investment. TSA's resources and personnel directly support ongoing security programs with committed security partners who, in turn, dedicate millions of private sector dollars to secure critical infrastructure, provide uniformed law enforcement and specialty security teams, and conduct operational activities and deterrence efforts. TSA invests its resources to help these partners identify vulnerabilities and risks in their operations, and works with specific owners/operators to develop and implement risk-mitigating solutions to address their specific vulnerabilities and risks.

Question 3. How will the cuts impact surface transportation security?

Answer. *Canine Team.* When discussing canine security teams, former TSA Administrator Neffenger said that "there is no better overall detector of explosives than a dog's nose" and that they "work an environment like no technology can."

Question 4. What benefits have you seen from the use of canine teams?

Answer. Canine teams are a highly mobile, reliable, and effective tool when properly trained and utilized. The benefits derived from all of our canine teams across all modes of transportation (Aviation, Surface, Maritime and PSC) is immeasurable. From providing a clearly visible deterrent, to their unmatched detection capabilities, to the many and varied environments in which they operate, the presence of a well-trained canine team has proven to significantly enhance the overall security footprint.

Question 5. How would funding for additional teams help improve security?

Answer. Increasing the number of canine teams would not only provide for greater coverage and additional detection capability in the transportation network, but also directly increases the deterrence factor, possibly altering or preventing a terrorist attack.

Question 6. Are there other ways that the Federal Government can help incentivize the use of canine teams?

Answer. TSA maintains a list of current law enforcement participants who have requested to increase their current canine team allocation, as well as non-participating agencies that have requested to join TSA's National Explosives Detection Canine Team Program (NEDCTP). Most agencies do not have sufficient discretionary funding to support an increase in their current canine allocation or to establish a canine program, and therefore appeal to the Federal Government for assistance. The TSA program currently covers the costs associated with the procurement of canines, handler training, yearly evaluations/certifications of teams and provides participants a $50,000 per team, per year reimbursement stipend. All other costs related to maintaining and operating the canine are the responsibility of the participant. In return, the participant agrees to spend 80 percent of their duty time in their assigned area of responsibility conducting explosive detection activities. One alternative solution is for TSA to stop providing the $50,000 stipend and for participants to bear all costs associated with maintaining and operating the canine teams. TSA would still provide the canines, explosives training aids, handler training, and yearly evaluation/certification of the teams.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. MARIA CANTWELL TO HON. DAVID P. PEKOSKE

Port Security Grant Program. America's seaports and airports must be prepared to face a wide range of threats and vulnerabilities, both natural and manmade. Yet the Port Security Grant Program, in which TSA is a partner, and other Federal programs that support ports' efforts are limited to preventing terrorist and criminal activity or providing assistance after an emergency has already occurred.

More and more, security experts are advocating for an all-hazards approach to protecting our citizens and critical infrastructure. Such an approach seeks to prevent a wider range of potential threats and to make our communities more resilient when incidents occur.

Question. To your knowledge, is DHS considering adjusting its practices to reflect this evolving consensus port security and threat management? Would you agree that there would be value in introducing more flexibility into the Port Security Grant Program to accommodate an all hazards approach?

Answer. The Port Security Grant Program (PSGP) is administered by the Federal Emergency Management Agency (FEMA) in accordance with the legislative requirements of 46 United States Code (USC) 70107.

Specifically:

(b) Eligible Costs.—The following costs of funding the correction of Coast Guard identified vulnerabilities in port security and ensuring compliance with Area Maritime Transportation Security Plans and facility security plans are eligible to be funded:

(1) Salary, benefits, overtime compensation, retirement contributions, and other costs of additional Coast Guard mandated security personnel.

(2) The cost of acquisition, operation, and maintenance of security equipment or facilities to be used for security monitoring and recording, security gates and fencing, marine barriers for designated security zones, security-related lighting systems, remote surveillance, concealed video systems, security vessels, and other security-related infrastructure or equipment that contributes to the overall security of passengers, cargo, or crewmembers. Grants awarded under this section may not be used to construct buildings or other physical facilities, except those which are constructed under terms and conditions consistent with the requirements under section 611(j)(8) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5196(j)(8)), including those facilities in support of this paragraph, and specifically approved by the Secretary. Costs eligible for funding under this paragraph may not exceed the greater of—

(A) $1,000,000 per project; or

(B) such greater amount as may be approved by the Secretary, which may not exceed 10 percent of the total amount of the grant.

(3) The cost of screening equipment, including equipment that detects weapons of mass destruction and conventional explosives, and of testing and evaluating such equipment, to certify secure systems of transportation.

(4) The cost of conducting vulnerability assessments to evaluate and make recommendations with respect to security.

(5) The cost of conducting exercises or training for prevention and detection of, preparedness for, response to, or recovery from terrorist attacks.

(6) The cost of establishing or enhancing mechanisms for sharing terrorism threat information and ensuring that the mechanisms are interoperable with Federal, State, and local agencies.

(7) The cost of equipment (including software) required to receive, transmit, handle, and store classified information.

(8) The cost of training law enforcement personnel—

(A) to enforce a security zone under section 70132 of this title; or

(B) assist in the enforcement of a security zone.

The legislation primarily directs the program to provide security related capabilities. Funding priorities under the PSGP are continually informed by risk and threat assessments provided by the United States Coast Guard (USCG), as the lead Federal agency for maritime security. Having USCG as lead ensures that the program is flexible in evolving to reflect the most current maritime security risks facing American ports and waterways. TSA defers to the USCG, as the lead for Maritime Security, regarding introducing more flexibility in the PSGP to accommodate an all hazards approach, however many security mitigation/response capabilities are by nature all-hazards in nature.

Note: On May 21, 2018, FEMA released the Notice of Funding Opportunity and allocations for the Port Security Grant Program. In FY 2018, the PSGP provides $100,000,000 for transportation infrastructure security activities to implement Area Maritime Transportation Security Plans and facility security plans among port authorities, facility operators, and State and local government agencies required to provide port security services. The intent of the FY 2018 PSGP is to competitively award grant funding to assist ports in obtaining the resources required to support the development and sustainment of core capabilities identified in the National Preparedness Goal of a secure and resilient Nation.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RICHARD BLUMENTHAL TO HON. DAVID P. PEKOSKE

Whether TSA has technology ready to deploy that can detect explosives at rail and transit stations. In recent weeks, we have been tragically reminded of the security threats facing our rail and transit network.

On December 11, 2017, a terrorist detonated a homemade pipe bomb affixed to his torso with the aim of inflicting as much death as possible in a New York City subway station. Fortunately, the bomb only partially detonated, no one was killed, and injuries were at a minimum.

TSA must take action to protect critical transportation hubs immediately—like rolling out non-invasive technology that can find and detect concealed explosives by identifying objects that block the natural emissions from a person's body.

I understand that this technology is being tested in Los Angeles, and some of my colleagues have publicly wondered whether it can be deployed.

I urge you to expedite the testing process to ensure its efficacy so this technology can be deployed nationally. It is critical that we ensure safety without imposing any unnecessary screening burdens on passengers.

Question 1. What is the status of this technology? When will it be ready for use and deployment? Can you confirm that you're working to roll out technology without imposing any unnecessary new screening burdens?

Answer. TSA continues to collaborate with the technology marketplace to gain new capabilities and enhance existing ones. Two vendors have systems proven to be effective and suitable when used in accordance with their known capabilities and limitations and with appropriate concepts of operations. TSA has completed its assessment of the two systems and they are ready to be purchased by appropriate users directly from the vendors. The local and regional surface transportation systems, privately owned and operated, are the appropriator buyers and users of the technology. TSA will continue to seek improvements and expand capabilities of this type of technology. Several major transportation systems are expressing an interest in either applying for grants funding to purchase or purchasing with their own capital funds.

Checkpoint style screening is not feasible in high volume mass transit/passenger rail environments. The technologies are designed to accommodate high volumes of passengers moving in diverse directions without unnecessarily impeding passenger flow.

TSA is continuing its programs energizing the marketplace to provide security technologies that meet the needs of the surface transportation industry.

Question 2. When and if the technology is ready and helpful—not harmful—can you commit to putting it in commuter rail, not just subways?

Answer. TSA provides assessments and testing/pilot data and information in order to verify technology. This data and testing can assist in drafting of grants proposals and industry procurement decisions of technology for surface security. TSA is not funded to procure or field security technologies for the surface transportation industry. That includes both subways and commuter rail. Industry purchases technology directly from the marketplace or through the various Federal grant programs.

The need to address the growing menace of terrorists, trucks and "vehicle ramming incidents". In recent years we've seen a growing menace: terrorists getting hold of large trucks and vans and using them as weapons to kill and maim many.

Perhaps the most high-profile was the attack in France in 2016 in which 86 were killed. But there have been many others, for instance:

In June 2017, terrorists used a van to kill pedestrians on London Bridge, killing eight.

In August, a terrorist used a van to drive over pedestrians in Barcelona, killing 14.

In October, close to home, a terrorist used a truck to drive over pedestrians in New York City, killing eight.

Question 3. I asked about this issue at your confirmation hearing in June. I recall your having said that you would look at this very closely. What efforts have you made to address this issue? How are you addressing these terrifying scenarios?

Answer. The Department of Homeland Security's (DHS) Office of Operations Coordination collects information on more than 15,000 special events annually and performs a comparative risk analysis to assess the likelihood of a terrorist attack at these events. The results of this objective analysis are used across the Federal Government for situational awareness and to make policy decisions about how to support state, local, tribal, and territorial authorities. Higher risk events may re-

ceive support from DHS and other Federal agencies. For example, DHS's field-based Protective Security Advisors (PSAs) serve as security subject matter experts who engage with state, local, tribal, and territorial government mission partners and members of the private sector stakeholder community to protect the Nation's critical infrastructure. When directed, PSAs work with venue managers to mitigate their security vulnerabilities, which includes the threat of a vehicle ramming scenario.

DHS is in the process of establishing a comprehensive program specifically focused on the security of soft targets-crowded places. The focus of the program is to develop and implement innovative solutions to reduce the probability of a successful attack by adversaries who may be utilizing a variety of tactics, from simple methods to more sophisticated weapons. The program will include the development of enhanced security protocols, standards, guidance, technology, and security-by-design approaches.

As part of this effort, continuing with existing authorities and requirements, the Department's National Protection and Programs Directorate (NPPD) is expanding upon its capabilities to assist the critical infrastructure community in mitigating risks associated with vehicle ramming attacks through a variety of means:

Protection Operations: In May 2018 the Federal Protective Service (FPS) implemented its concept of operations for the protection of Federal facilities identified as soft targets and crowded places that are located adjacent to or near Federal facilities (sports venues, bus, subway and train transit hubs, etc.) across the United States. Formally known as Operation Resilient Protection (ORP), these operations provide enhanced law enforcement, intelligence analysis, criminal investigations, and physical security for pre-selected soft targets and crowded places. Additionally, FPS implements ORP at Federal facilities during NSSEs, and SEAR Levels I, II, and III. ORP was specifically developed and implemented in response to international and domestic incidents of vehicle ramming, mass shootings, sniper attacks, and other terrorism-related tactics affecting soft targets and crowded places. Furthermore, in partnership with the General Services Administration, FPS also conducts Operation Reduce Risk, a program to identify, interdict and recover counterfeit, stolen and lost government license plates reducing the likelihood that an official looking vehicle can gain access to be used in a vehicle based attack.

Partnership: As the executor of the Commercial Facilities Sector-Specific Agency responsibilities, NPPD expanded its partnership base to more effectively address vehicle ramming impacts to commercial facilities. The American Car Rental Association (ACRA) and the Truck Rental and Leasing Association (TRALA) are working closely with NPPD to identify methods of enhanced security measures, which may reduce the vulnerability of rental vehicles being used for attacks. These partnerships include coordination with the Transportation Security Administration (TSA) and Federal Bureau of Investigation (FBI). As Task Force Officers assigned to FBI Joint Terrorism Task Forces across the United States, FPS criminal investigators continually partner with the FBI and state and local police and sheriffs' departments. FPS uniformed police officers and commanders routinely partner with state and local police and sheriffs' departments to protect Federal facilities from vehicle ramming and other terrorism-related tactics.

Exercises: NPPD incorporates vehicle ramming attacks into exercise scenarios conducted with the critical infrastructure community. These exercises provide the opportunity to test response protocols along with pre-incident information sharing processes, emergency response plans, and recovery procedures involving soft targets-crowded places. So far in Fiscal Year (FY) 2018, NPPD has conducted 14 tabletop exercises with public and private sector stakeholders that included vehicle ramming as part of the scenarios.

Resources: In February 2018, NPPD produced a "Vehicle Ramming Attack Mitigation" video, which provides information to assist the critical infrastructure community in mitigating this evolving threat with technical analysis from public and private sector subject matter experts. The video leverages real-world events, and provides recommendations aimed at protecting organizations as well as individuals against potential vehicle ramming incidents.

Intelligence Bulletin: In November 2017, FPS released a revised Operational Readiness Bulletin (ORB) to all assigned law enforcement officers, providing guidance regarding strategies, tactics, techniques, and procedures for mitigating vehicle ramming attack vulnerabilities. In December 2017, FPS released an Intelligence Bulletin that provided an in-depth study of criminal and terrorist vehicle ramming incidents, highlighting terrorist attack tactics, indicators to recognize developing incidents, and countermeasures to mitigate the effects of vehicle ramming attacks. NPPD also used analysis of Foreign Terrorist Organization-inspired vehicle ram-

ming operations in the west since 2016 to develop a product that informed the critical infrastructure community on common characteristics of these operations, and recommended mitigation strategies to improve resilience against future attacks. FPS routinely publishes intelligence bulletins related to vehicle ramming and other terrorism-related tactics. Depending on information classification, the bulletins are provided to partner intelligence and law enforcement agencies, Federal Executive Boards, and Federal agency leaders.

Webinars: NPPD conducted two webinars in 2017. The soft targets-crowded places webinar provided an overview of select attacks and corresponding tactics, techniques, and procedures. In attendance were 1091 registrants from the Critical Infrastructure Sector as well as representatives from Federal and local governments and the private sector. The second webinar focused on vehicle ramming, leveraging the information within the intelligence product mentioned above. This webinar was attended by 441 registrants from the Critical Infrastructure Sector as well as representatives from Federal and local government and private sector.

Resource Development: To raise awareness in the commercial vehicle industry, TSA worked with public and private sector partners to develop an informational product on vehicle ramming attacks released in June 2017. This product included information on the threat landscape, indicators, and countermeasures that could be implemented to prevent and prepare for this evolving threat. This document is scheduled to be updated in May 2018.

Preventive Measures: Although TSA's primary focus is on transportation security, it also coordinates with public and private sector partners to develop physical security measures to prevent vehicle ramming attacks against soft targets. This includes scenario-driven security exercises and the implementation of physical security countermeasures to protect mass gatherings at public events. In April 2018, TSA facilitated a vehicle ramming seminar at the Kentucky Department of Criminal Justice Training with the Kentucky State Police (KSP) and Kentucky Trucking Association. This seminar focused on intelligence briefings, a table-top-exercise with a vehicle ramming scenario, and a live demonstration by the KSP, Metro SWAT, and the State Bomb Squad to exercise response to a vehicle ramming attack. TSA is in discussions with other state level associations and law enforcement agencies to replicate this effort. TSA is currently working with the American Trucking Association and state associations in New York and Tennessee to conduct up to three full-scale exercises in FY2019. FPS recently developed and is testing a risk analysis modeling tool to determine the most effective risk-reduction physical security measures and protection activities relative to vehicle ramming and terrorism-related tactics. Validation of this methodology will continue through Fiscal Year 2019.

Security Information Sharing: TSA collaborated with ACRA and TRALA to share relevant security information to prevent the use of rental vehicles in vehicle ramming attacks. Through this partnership, TSA and the industry developed a report, titled "Security Indicators for the Vehicle Rental Industry," which was released in August 2017 to nearly 500 public and private stakeholders who have further distributed the messages within their industries and communities. TSA also leverages ongoing engagement opportunities, including webinars, meetings, and industry conferences to promote vehicle security and countermeasures against vehicle ramming attacks, to reduce the likelihood and consequences of vehicle ramming events. Additionally, TSA continues to promote security through Security Awareness Messages and industry calls surrounding worldwide attacks, including vehicle ramming, to address the ever evolving threat landscape, current tactics being deployed, and potential countermeasures. In February 2018, TSA hosted a Public Area Security Summit to discuss ways to mitigate the risk to public areas, including the risks from vehicle ramming attacks. Attendees included stakeholders from domestic and international surface transportation industry, aviation industry stakeholders, and other Federal agencies.

The significance of protecting ports. As you likely know from your Coast Guard experience—including many years in Connecticut, the U.S. has more than 1,000 harbor channels and 25,000 miles of inland, intra-coastal, and coastal waterways that serve over 360 ports.

U.S. seaports handle more than two billion tons of domestic, import and export cargo annually.

TSA has an important role in port security. Connecticut has three ports—which are vital to our economy, just like our country's hundreds of other ports.

Question 4. How secure is our maritime economy? What else can we do to ensure our ports are as secure as they need to be?

Answer. In contrast to the other surface modes of transportation, the Transportation Security Administration (TSA) is not the lead Federal agency for security in the maritime mode. The United States Coast Guard (USCG) is the lead Federal agency for maritime security in the United States, and TSA supports the USCG in its maritime security efforts and in coordinating interagency efforts for the maritime mode.

TSA supports the USCG in maritime security via the jointly administered Transportation Worker Identification Credential (TWIC) program. For the TWIC program, TSA conducts a security threat assessment of individuals who are seeking unescorted access to secure areas of maritime facilities and vessels. The assessment includes recurrent vetting against intelligence databases for ties to terrorism, fingerprint-based criminal history records checks, and an immigration status check. TSA issues a biometric credential to the individuals who successfully complete this process. While the USCG manages the physical access requirements and the associated enforcement and usage of the TWIC at the ports as part of USCG's overall maritime security mission, TSA and USCG jointly manage an enforcement program to ensure that only properly vetted personnel are entering secure areas of port facilities. TSA prioritizes High Threat Urban Areas. In Fiscal Year (FY) 2017, TSA Inspectors visited U.S. port facilities 1,695 times and inspected 59,790 TWICs. As a result, 180 Civil Enforcement Actions were taken, resulting in 67 fines and 113 warning letters. In FY 2018 to date, TSA Inspectors have visited U.S. port facilities 1,085 times and inspected 36,849 TWICs. TSA exceeded its target for inspections in FY 2017, so far for FY 2018, and continues to increase its targets.

How a passenger with neither a ticket nor passport was able to glide past security checkpoints and fly from Chicago to London. I understand this hearing concerns surface transportation security—an issue I want to be sure we address.

But I would be remiss if I didn't raise an issue that rightfully garnered significant headlines over the past week.

The headlines concerned an individual named Marilyn Hartman—apparently well-known to law enforcement officials in the aviation community. According to reports and statements from police and security officials, she was able to get past security officials at O'Hare in Chicago and onto a flight bound for London, where she landed before being apprehended and flown back to the U.S. last week.

No one was hurt. And her efforts raise concerns as well about mental health.

But nonetheless the episode raises very serious concerns about glaring, gaping holes in TSA's oversight. It gives me tremendous pause and makes me nervous about what someone with more nefarious motives could achieve.

Question 5. How do you respond to this incident? Does it worry you as much as it worries me? What steps have you taken to make sure it never happens again? How can we be sure it will not recur?

Answer. The incident at O'Hare International Airport (ORD) was investigated and lapses in security procedures were discovered both at the checkpoint and at the boarding gate. At ORD, physical barriers were added and ticket document checking locations were repositioned for optimal viewing of passengers. TSA worked with stakeholders to address other lapses in security procedures. An after action meeting of all law enforcement entities, airport authorities and air carriers was conducted on

February 5, 2018 to finalize changes and ensure success in the future. These efforts proved effective when Ms. Hartman was detected and arrested at ORD shortly after being released from custody following the first incident in question. Additionally, a different individual was detected and arrested at ORD when that subject attempted to bypass the Travel Document Check position.

TSA continues to provide training and national briefings on the importance of area security to prevent future incidents like this. We also routinely conduct inspections and testing during the airline boarding process to ensure that the proper security procedures are in place. While there is no guarantee that this type of incident will not occur again, the specific efforts taken at ORD, incorporation of lessons learned in national guidance and training, and inspection regime should reduce the likelihood of recurrence.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. EDWARD MARKEY TO HON. DAVID P. PEKOSKE

Transit Security Grant Program. When it comes to surface transportation security, we need a layered approach—technology, personnel, canines, public engagement. An all the above strategy.

That's why Congress established the Transit Security Grant Program, which provides transit systems with Federal resources to protect critical surface transportation infrastructure and the traveling public from acts of terrorism.

But since 2009, funding for this critical program has been slashed by over 80 percent, putting a tremendous strain on our public transit systems to address national security threats.

Question 1. Administrator Pekoske, would our transit systems be better able to address surface transportation security threats if Congress provided more funding for the Transit Security Grant Program?

Answer. The Department of Homeland Security's (DHS) Transit Security Grant Program (TSGP), administered by the Federal Emergency Management Agency (FEMA), is an instrumental component of public transit systems' security programs. The Transportation Security Administration (TSA) works very closely with FEMA to ensure that the TSGP funding priorities and framework are structured to buy-down the most risk.

In FY 2018, the Transit Security Grant Program (TSGP) provides $88,000,000 to the Nation's High-Threat Urban Areas for enhancement of security measures at critical transit infrastructure including bus, ferry, and rail systems. The intent of the FY 2018 TSGP is to competitively award grant funding to assist transit systems in obtaining the resources required to support the development and sustainment of core capabilities identified in the National Preparedness Goal of a secure and resilient Nation.

As your question notes, we need a layered approach to security to protect our Nation's surface transportation systems from terrorist threats. While TSGP funding is an important component in many transit systems' approach to security, we must focus on the ways in which the security layers fit and work together instead of on one layer in and of itself. Effective security projects, including those funded through the TSGP, are the result of several activities, many of which TSA helps support at no cost to transit systems. Security projects should be based on a threat and vulnerability assessment and tied into a security planning process, as TSA's Baseline Assessment for Security Enhancement (BASE) program helps public transportation systems accomplish; the BASE program is a voluntary security assessment of national mass transit and passenger rail MTPR that informs development of risk mitigation priorities and helps influence TSA allocations and resources. Projects can also be the result of lessons learned and areas for improvement identified in exercise After Action Reports, such as those from TSA's Intermodal Security Training and Exercise Program (I–STEP), which provides exercises, training, and security planning tools to public transportation agencies to strengthen company security plans, policies and procedures, and the Exercise Information System online tool.

The threat environment is ever-changing, and TSA puts a priority on disseminating intelligence information to appropriate entities through monthly industry conference calls, and via "as-needed" calls when real-life events occur.

Canine Teams. Man's best friend is also one of our greatest allies in our efforts to defeat terrorism at home.

The MBTA—Massachusetts Bay Transportation Authority—has eight canines.

But we need more than eight canine teams to protect the Nation's fourth largest transit system, with 145 rail stations and 177 bus routes.

Question 2. Administrator Pekoske, will you work with me to ensure we address the MBTA's canine needs? What steps can we take to ensure we are providing our transit agencies and airports with the canines they need to address security threats?

Answer. TSA continually performs risk analyses on the transportation network and maintains a list of participating state/local agencies who request additional canine team allocations. In addition, TSA tracks all requests from agencies that are not a participant in TSA's Canine Program but have expressed interest in joining this voluntary program. In both cases, TSA strives to provide canine team allocations as funding permits.

MBTA has played a critical role in the TSA Canine Program since 2005, when they were first allocated three canine teams. Over time, TSA has been able to increase MBTA's canine team allocation.

TSA is funded for 1,047 canine teams, (372 proprietary teams and 675 state and local canine teams) all of which are currently assigned to specific participants. One measure TSA is looking at to expand the canine program is to offer participating state/local agencies the ability to increase the number of canine teams they deploy through the following proposal: TSA would provide the canines, explosives training aids, handler training, and yearly evaluation/certification of the teams; however, TSA would not provide the $50,000 per team stipend currently allotted to program

participants. The participant would bear all costs associated with the care and maintenance of the canine team.

Due to the continued demand for canines, TSA has been working to increase capacity in both training and fielded teams. TSA is piloting new training models, adding a new procurement contract to purchase canines with varying levels of training to assist in meeting future needs, and working closely with the Department of Defense Military Working Dog School to expand capacity at the Joint Base San Antonio-Lackland facility. TSA is committed to supporting our transit agencies and airports with the canines they need to address security threats.

Vehicle Ramming Attacks—Protecting Public Spaces. In recent years, terrorists have added another weapon into their arsenal—large vehicles.

Whether it be a promenade in France, a bridge in London, or a bicycle path in New York, terrorists have launched vehicle ramming attacks to kill hundreds and instill fear.

Administrator Pekoske, Massachusetts has many wonderful public spaces where my constituents congregate.

Question 4. How can we maintain the accessibility these public spaces while also protecting the public from vehicle ramming attacks?

Answer. The cornerstone of our thriving democracy is an open society that provides the means to freely engage in many activities without the fear of harm. Recent events such as vehicular attacks on pedestrians and shootings in schools, nightclubs, and at concerts; exemplify the importance of enhancing security at soft targets and crowded places. Protecting these areas from terrorists and other extremist actors, who are more prominently leveraging low sophistication attack methods, such as vehicle-ramming attacks to cause mass casualties, is a challenge that the department is meeting directly and forcefully.

The DHS National Protection and Programs Directorate (NPPD) is at the forefront of soft targets-crowded places efforts. In January 2018, the Department developed a plan to support and strengthen direct security operations, intelligence and information sharing, capability and capacity building, and research and development.

NPPD is also assisting the critical infrastructure community in mitigating risks associated with vehicle ramming attacks through a variety of means. Protective Security Advisors support security planning in coordination with federal, state, local, and private sector partners. They frequently conduct security assessments, coordinate training, and provide situational awareness of critical infrastructure in public gathering locations.

Vehicle Ramming Attacks—Technology. Technology can be part of the solution.

In 2016, a vehicle ramming attack in Berlin was eventually stopped when the truck's automatic braking technologies were triggered.

These safety innovations intervene when a collision is imminent, taking control of the brakes to avoid crashes.

While the European Union requires automatic braking systems on large trucks, the United States has not mandated that these life-saving technologies be adopted by larger vehicles.

Question 5. Administrator Pekoske, could broader adoption of automatic braking technologies help address the threat posed by vehicle ramming attacks?

Answer. Technologies now making their way into the vehicle industry could reduce the frequency and consequence of vehicle ramming attacks. The Transportation Security Administration supports further research into collision avoidance and other emerging technologies that may mitigate this risk.

We stand ready to work with our Federal partners at the Department of Transportation and the National Highway Traffic Safety Administration as they set standards for future safety devices and technologies for collision avoidance and remote vehicle disabling technologies.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO HON. DAVID P. PEKOSKE

Aviation. While I know you were both before the Committee to discuss surface transportation security specifically, I wanted to note that in October 2017, Mr. Kelly's office completed audits of several of TSA's most critical aviation security programs. The results of those audits are classified so I will not go into them further here, but I wanted to underscore just how seriously I and my colleagues take such reviews and the urgent importance of TSA running state of the art security programs across all modes of transportation.

As we all saw recently, a woman by the name of Marilyn Hartman successfully boarded a flight in Chicago without a ticket. She managed to make it all the way to London before she was stopped. Worse yet, she has successful boarded planes without a ticket multiple times since 9/11.

These security breaches have also impacted flights coming into Nevada. In 2013, a 9-year old boy managed to board a flight in Minneapolis and fly all the way to Las Vegas without being stopped.

Question 1. Administrator Pekoske, you spoke in your testimony about innovation. Can you outline the specific programs and processes your Administration have put in place to ensure TSA is regularly reviewing its standard operating procedures in both ground and aviation transportation systems to ensure state of the art practices? Are there other processes your organization has identified that would ensure TSA is using resources to maximize efficacy and adopt global best practices in transportation security?

Answer. The Transportation Security Administration (TSA) has implemented a Standard Operating Procedures (SOP) Review, Impact Analysis, and Maintenance Plan, which provides guidance and direction for the review and impact analysis process for SOPs. Reviews are recurrent (annually, semi-annually, or quarterly) and also conducted as-needed to ensure procedures align with or responds to current security policies and the evolving threat environment. The SOP review process includes reviewing intel-based requirements, new technologies, test outcomes, and audit recommendations, to improve overall detection and performance.

The review process was first implemented in August 2017. Since that time, as it relates to identity verification, the Travel Document Check SOP was updated and released on September 28, 2017 with an implementation date of October 12, 2017. Additionally, another interim change was released on January 22, 2018 with an implementation date of February 5, 2018. Both SOP releases supported the need for policy updates based on law making requirements (REAL ID) and identified areas of required clarification for the frontline workforce.

Hiring/Recruitment.

Question 3. We have seen with Customs and Border employment that recruitment can be a challenge. Have you seen similar barriers to bringing in qualified personnel who stay long enough to keep a consistent and high-level team together on both aviation, as well as surface transportation security?

Answer. Yes, with regard to our Transportation Security Officer (TSO) positions, TSA experiences many challenges in attracting and retaining qualified personnel as the compensation level of the TSO position is considerably lower than other positions in the field of homeland security. As the U.S. economy has improved and local minimum wages have substantially increased in recent years, the pay of the TSO position is becoming less and less competitive. In an effort to recruit quality applicants, we are doing our best to market the benefits of Federal employment.

To align with airline flight schedules, TSA is required to hire thousands of part-time TSOs each year. Hiring part-time employees with schedules of 20–25 hours per week poses challenges as many employers are currently offering full-time positions at comparable or higher starting hourly wages. In many instances, we are losing quality TSOs to other full-time jobs that offer the same, or sometimes, lower hourly rates. Thus, we try to adjust our recruitment and advertising to reach ideal part-time applicant pools, such as individuals who are going to school and in need of part-time employment.

More recently, we have seen a significant increase in the number of TSOs that have left TSA to transfer to other Federal agencies such as: data entry clerks for United States Citizenship and Immigration Services, call center agents for Federal Emergency Management Agency, and claims processors at the VA. For many, these entry-level positions at other agencies are promotions and typically offer traditional schedules without requiring early morning/evening/weekend/holiday shifts or needing to be flexible with personal schedules due to the TSO position being designated as emergency essential.[1] For what is considered an entry-level position, a great deal is expected and required from our TSOs.

TSA always looks to build on the strengths of our employees and advance their profession. TSA has created a road map for career progression that details the skills and certifications an officer needs to advance in their TSA careers. This roadmap provides a structured progression for officers to see their career trajectory,

[1] Emergency essential personnel are not excused from duty if an emergency arises because the employee encumbers a position that is identified as necessary to sustain a facility or function for continuity of TSA operations during an emergency.

incentivizes on-the-job expertise in critical areas, and helps the agency retain our highest skilled workers.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. DEB FISCHER TO JOHN V. KELLY

Question. Mr. Kelly, as you noted in your testimony, the background check process for the TWIC program is the same as that for aviation workers and the Hazmat Materials Endorsement. The Surface and Maritime Transportation Security Act would reduce duplicative background checks by allowing a person who has been approved for a TWIC credential to also be considered to have met the requirements for a hazardous materials endorsement. Would removing duplication across these credentials improve the effectiveness of the background check process for transportation facility access?

Answer. The Hazard Materials Endorsement (HME) is a state driver's license endorsement. The Transportation Security Administration (TSA) performs the background check to ensure consistent background check reviews across state lines. Based on our audit, we learned that TSA has already taken into consideration and adjusted its fees for individuals with the need for both a TWIC and an HME endorsement. According to TSA, applicants with HMEs do not have to repeat the security threat assessment if they are applying for a TWIC, and as a result the fee for the TWIC is reduced. Eliminating the requirement for additional background checks may not impact the effectiveness of the background check process because in most cases individuals who have received a TWIC will be automatically processed by TSA's system in less than one day. Since HME is a state generated endorsement we do not have jurisdiction to review the endorsement or its processes.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. BILL NELSON TO JOHN V. KELLY

Customs and Border Protecting Staffing at MCO. Mr. Kelly, I have been told by the Orlando International Airport that U.S. Customs and Border Protection (CBP) officers there are being reassigned to the Southwest border as part of a continuing rotation.

Question. Has your office been made aware of these rotations and can you comment on why it is necessary to shift resources from ports of entry already experiencing C.B.P. staffing shortages?

Answer. We are not aware of any specific rotations from Orlando International Airport to the Southwest border. As part of an ongoing audit, we have received information which indicates CBP's Office of Field Operations has fallen short of its staffing targets for Fiscal Year (FY) 2016, FY 2017, and FY 2018. According to CBP, it is working to address the shortages.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RICHARD BLUMENTHAL TO JOHN V. KELLY

The need for an aggressive, extensive review of the administration's handling—or mishandling—of Puerto Rico recovery efforts. I understand this hearing concerns surface transportation security, an issue with critical importance in Connecticut. I want to briefly mention another issue while the DHS IG is with us here today.

I'm proud to represent the state with the highest concentration of Puerto Ricans in the U.S. In the days after the hurricane, my constituents and I grew very concerned over FEMA's oversight of the recovery. Our concerns remain.

I've now been to Puerto Rico twice since Hurricane Maria hit. I have seen little real, robust progress. As I wrote in October to the DHS IG, the American people need to know whether the Trump administration is truly focused on helping the millions of Americans now suffering in Puerto Rico.

Question 1. What steps is your office taking to investigate the effectiveness of the response in Puerto Rico?

Answer. In my recent trips to Puerto Rico, I also witnessed first-hand the devastation and hardship that Hurricane Maria caused to the citizens of the United States that call Puerto Rico home. When Hurricane Maria hit Puerto Rico, our office's first order of business was to deploy auditors and investigators to FEMA's Joint Field Office in Puerto Rico. Currently, we have four auditors and five investigators in Puerto Rico. Having Office of Inspector General (OIG) staff on the ground serves

multiple purposes: to serve as an independent unit for oversight of disaster response and recovery activities; to detect and alert FEMA of systemic problems; and to help ensure accountability over Federal funds. We focus our deployment activities on identifying potential risks and vulnerabilities and providing our stakeholders with timely, useful information to address emerging challenges and ongoing operations.

Specifically, our auditors have begun, or are planning, a variety of reviews both at the Federal and local level, intended to improve FEMA's programs and operations. For instance, we plan to start capacity audits in Puerto Rico during this Fiscal Year. Capacity audits and early warning audits identify areas where FEMA public assistance grant recipients and sub-recipients may need additional technical assistance or monitoring to ensure compliance with Federal requirements. By undergoing an audit early in the grant cycle, grant recipients and sub-recipients have the opportunity to correct noncompliance before they spend the majority of their grant funding. It also allows them the opportunity to supplement deficient documentation or locate missing records before too much time elapses.

The other audit work we have underway or planned in Puerto Rico focuses on a range of issues, including:

- challenges with providing Puerto Rico disaster survivors roof coverings to reduce further damage to their homes and property;
- review of disaster-related contracting including the contracts with Whitefish Energy, Cobra Acquisitions, Bronze Star LLC (blue tarps) and Tribute Contracting LLC (meals), among others;
- additional controls for Puerto Rico's high-risk grant applicants;
- FEMA's preparedness, management, and distribution of supplies;
- lessons learned from repair versus replacement funding decisions;
- FEMA's plan to use alternative procedures for the Public Assistance Program;
- police overtime pay;
- Federal considerations relating to the privatization of the Puerto Rico Electric Power Authority;
- duplication of Federal benefits (in coordination with HUD OIG); and
- key infrastructure repair costs (such as for the Guajataca Dam).

We will continue to work with FEMA, its partners, and our oversight community to help ensure challenges are timely identified and addressed.

With respect to our investigative work, our law enforcement investigators' efforts in Puerto Rico have already yielded results, uncovering serious schemes aimed at defrauding FEMA and turning disaster survivors into victims. For example:

- We are investigating a widespread identity theft ring in which numerous individuals used the stolen identities of hurricane victims to fraudulently apply for benefits, thereby defrauding FEMA and victimizing hurricane survivors.
- We have arrested an individual—in coordination with U.S. Immigration and Customs Enforcement—for False Impersonation of a Federal Officer or Employee. This individual attempted to procure work at an Emergency Management Center as a voluntary staff member for Hurricane Maria relief efforts. At the time of the arrest, the individual was wearing a Homeland Security Investigations Special Agent t-shirt, a DHS cap, and had a fake DHS badge in his possession. Our agents obtained consent to search the person's residence where they found additional t-shirts with Homeland Security Investigations logos.

We will continue to review and triage the many complaints and allegations that we receive each day, and judiciously expend our limited investigative resources on those matters that pose the greatest threats or risks to FEMA programs and operations. We will conduct our investigative work in close and timely coordination with our investigative partners, FEMA, and our oversight community with the aim of protecting disaster survivors and the billions of taxpayer dollars entrusted to the critical efforts of disaster response and recovery.

Question 2. When will we see a final investigative report?

Answer. With respect to our audit work, we anticipate finalizing audit reports on the following issues this summer:

- challenges with providing Puerto Rico disaster survivors roof coverings to reduce further damage to their homes and property;
- review of disaster-related contracting including the contracts with Bronze Star LLC (blue tarps) and Tribute Contracting LLC (meals); and
- additional controls for Puerto Rico's high-risk grant applicants.

We anticipate completing additional audit work in Puerto Rico by the end of the year.

With respect to our investigative work, while the results of our law enforcement investigative reports in Puerto Rico will not be made public, we would be happy to brief the Committee on our efforts once the investigations have closed.

The need for greater review of DHS' sensitive locations policy. Both CBP and ICE are bound by policies that enforcement operations should not be undertaken in sensitive locations such as churches, hospitals and schools, absent exigent circumstances. Nonetheless, there are widespread reports of violations of these policies.

I have led two letters to DHS asking to clarify DHS policies on sensitive locations and provide basic statistical data on compliance with existing DHS policy regarding sensitive locations. One letter was dated October 17, 2017, and the other was dated November 13, 2017.

The letters were driven by two particularly horrific reports of apparent violations of DHS policies regarding sensitive locations. Last May, CBP officers apprehended young parents Irma and Oscar Sanchez from a hospital while their baby awaited emergency surgery. In October, Rosa Hernandez, a 10-year-old girl with cerebral palsy, was detained by CBP on her way to the hospital.

Question 3. Are you reviewing DHS' flouting of these policies?

Answer. Although we do not have any past or ongoing work on this issue, our office is considering including an audit, inspection, or special review of DHS policies, training, and actions at or near sensitive locations to our Fiscal Year 2019 plan.

Question 4. Do you have any insight on whether that has been any disciplinary or accountability measures taken against the officers involved in those cases?

Answer. No, because we have not yet undertaken work in this area, we are not aware of any disciplinary or accountability measures the Department may have taken in connection with the cases you referenced.

Question 5. Do you have any insight into what measures are in place to ensure that ICE and CBP track enforcement actions taken in sensitive locations and document the exigent circumstances that justify them?

Answer. To the extent we initiate work on this issue, an evaluation of ICE and CBP's system for tracking enforcement actions in sensitive locations would likely feature in that review.

Question 6. Do you have any insight into training to ICE and CBP officers receive on the sensitive locations policy of the Department?

Answer. To the extent we initiate work on this issue, an evaluation of the training ICE and CBP officers receive on conducting enforcement actions in sensitive locations would likely feature in that review.

Recent DHS IG report on Trump's immigration order. The DHS IG released a long-awaited report on DHS' implementation of Executive Order #13769—the President's first Muslim ban. The report stated that DHS was totally unprepared for even the most basic and obvious consequences of the Muslim ban. In addition, the report found that CBP was aggressive in preventing affected travelers from boarding planes headed to the U.S., in violation of two separate court orders.

In a department memo issued on January 12—in anticipation of the release of the report—DHS management criticized the report, saying that it "contains a number of legal and factual inaccuracies and is methodologically flawed."

This report was completed months ago but was not publicly released until last week. Your predecessor, John Roth, resigned after saying he was troubled by attempts by the Department to redact information that would cast the Department's response in a negative light.

Question 7. Do you stand by the assertions and conclusions in this report?

Answer. Yes.

Question 8. Why did this report take months to be released in its entirety?

Answer. DHS OIG's standard process typically includes providing the Department an opportunity to review a draft report prior to publication to identify information the Department believes should be withheld from public release on the basis of, among other things, a statute or Executive Order mandating nondisclosure (*e.g.,* the Privacy Act). Pursuant to this standard process, a draft of the report in question was provided to the Department on October 6, 2017. Former Inspector General Roth requested that the Department complete its sensitivity review within two weeks of receipt. Just before the deadline passed, the Department advised DHS OIG that it had sensitivity concerns regarding the content of the report, but did not identify what portions of the report were potentially sensitive. Over the next few weeks,

DHS OIG engaged the Department in discussions regarding the Department's sensitivity concerns and proposed redactions.

As you are likely aware from Mr. Roth's November 20, 2017 letter to the congressional requestors of the review and related press release from our office, DHS OIG was troubled by the Department's delays in articulating its sensitivity concerns with respect to this report. Ultimately, the Department sought a privilege review by the Department of Justice and eventually provided a draft of the report with its final proposed redactions after close of business on Friday, January 12, 2018—more than three months after DHS OIG had provided the draft to the Department. The following Monday, January 15, was a Federal holiday. When business resumed on January 16, 2018, DHS OIG worked expediently to analyze and incorporate the Department's management response. We published the report on Thursday, January 18, 2018.

Question 9. Some information in the report has been redacted. Was any information redacted as a result of interference by Trump political appointees who sought to remove text that would have painted the Department in a negative light?

Answer. As noted above, DHS OIG's standard process typically includes soliciting input from the Department regarding information in draft OIG reports the Department believes is not subject to public release. Pursuant to this standard process, a draft of the report in question was provided to the Department in October 2017. The Department ultimately claimed privileges on various grounds, including deliberative process and attorney-client privilege. Although DHS OIG believes many of the Department's withholdings are overly broad and would not withstand judicial scrutiny, the Department has made what it claims to be good faith redactions pursuant to these privileges; accordingly, we are bound to publish the report with the Department's redactions.

Question 10. Do you stand by the report's finding that DHS was "largely caught by surprise by the signing of the [Executive Order] and its requirement for immediate implementation?"

Answer. Yes.

Question 11. Do you stand by the report's finding that the DOJ Office of Legal Counsel failed to analyze the due process rights of legal permanent residents or Special Immigrant Visa holders when it approved the Executive Order?

Answer. We did not review the DOJ Office of Legal Counsel's (OLC) process for approving the Executive Order, as DHS OIG does not have jurisdiction to review the actions of DOJ employees. Accordingly, we are not in a position to say whether DOJ OLC analyzed the due process rights of legal permanent residents or Special Immigrant Visa holders as part of its approval determination. Our report notes, however, that the memorandum DOJ OLC ultimately issued approving the Executive Order did not include any analysis of due process rights—in fact, it did not include any analysis at all to support the conclusion that the Executive Order was proper in terms of "form and legality." We stand by our report's description of DOJ OLC's memorandum.

Question 12. Do you stand by the report's finding that CBP did not detect "any traveler linked to terrorism based solely on the additional procedures required by the [Executive Order]"?

Answer. Yes, based on the information available to us at the time of our review, we stand by the report's finding that CBP did not detect "any traveler linked to terrorism based solely on the additional procedures required by the [Executive Order]."

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO JOHN V. KELLY

Aviation. While I know you were both before the Committee to discuss surface transportation security specifically, I wanted to note that in October 2017, Mr. Kelly's office completed audits of several of TSA's most critical aviation security programs. The results of those audits are classified so I will not go into them further here, but I wanted to underscore just how seriously I and my colleagues take such reviews and the urgent importance of TSA running state of the art security programs across all modes of transportation.

As we all saw recently, a woman by the name of Marilyn Hartman successfully boarded a flight in Chicago without a ticket. She managed to make it all the way to London before she was stopped. Worse yet, she has successful boarded planes without a ticket multiple times since 9/11. These security breaches have also impacted flights coming into Nevada. In 2013, a 9-year old boy managed to board a flight in Minneapolis and fly all the way to Las Vegas without being stopped.

Question 1. Mr. Kelly, where do you assess TSA stands in implementing some of the related recommendations you mentioned: creating a risk-based strategy and incorporating risk into its budgeting process?

Answer. TSA issued a 2018 National Strategy for Transportation Security (the Strategy) that purports to address the security of "transportation assets in the United States . . . from attack or disruption by terrorist or other hostile forces." The Strategy presents a base plan that outlines a risk-based foundation for the Strategy, and appends security plans that provide mode-specific and intermodal activities to reduce terrorism risks and to protect transportation systems. We continue to follow up with TSA on the implementation of its Strategy.

While TSA has taken steps to formalize its budgeting process, it still lacks a formal process to incorporate risk in its budget formulations. TSA guidelines do not currently direct TSA transportation modes to align resources with risk. Incorporating risk into the budgeting process would help TSA decision-makers align resources more effectively.

Question 2. Are there other processes your organization has identified that would ensure TSA is using resources to maximize efficacy and adopt global best practices in transportation security?

Answer. Through our hard-hitting audit work, which has resulted in numerous recommendations, we have attempted to direct TSA to adopt global best practices in transportation security. For example, during one of our audits, we found that TSA did not receive all terrorism-related information to vet aviation workers, and had multiple quality issues in the biographic data it used to vet those workers. In response to our report, TSA has implemented our recommendations with the effect of increasing the quantity and quality of information used for vetting.

We have also identified areas where TSA could utilize its resources more effectively. For instance, we recently identified limitations with the Federal Air Marshal Service (FAMS) contributions to aviation security. While details related to FAMS operations and flight coverage presented in our work are classified or designated as Sensitive Security Information, we identified a part of FAMS operations where, if discontinued, funds could be put to better use. In addition, we are drafting a report on our recent access control testing which will provide recommendations to the agency to strengthen access controls and security breaches.

Travel Ban for the DHS IG. Mr. Kelly, recently your office released a report on the implementation of Executive Order 13769, which is better known as President Trump's first attempt at implementing a Muslim Travel Ban. The report, prepared by your predecessor, concludes that Customs and Border Patrol was unprepared for the roll out of the travel ban, and that the resulting chaos harmed the agency's reputation. Further, although the report found that CBP agents at U.S. ports of entry made good faith efforts to comply with court orders blocking the executive order, there were still violations.

Although this report was completed in early October, it was only released in mid-January, reportedly because DHS and the Department of Justice slow-walked the sensitivity and privilege reviews.

Question 3. Mr. Kelly, when did your office learn that DHS and DOJ had completed their reviews?

Answer. On November 29, 2017, we learned that DOJ had completed its review. The Department has not shared a copy of DOJ's analysis with DHS OIG. On January 12, 2018, we received the Department's final redacted version of the report along with its official Management Response.

Question 4. Mr. Kelly, you've been with the Office of the Inspector General within DHS since 2008. In your experience, is it common for the Department of Homeland Security to claim deliberative process privilege in order to redact significant portions of a report by an Inspector General?

Answer. It is extremely rare for the Department to claim the deliberative process privilege to redact any portions of an Inspector General report. As former Inspector General Roth noted in his November 20, 2017 letter to Congress, this was the first time in his tenure as Inspector General that the Department had indicated it may assert this privilege in connection with one of our reports or considered preventing the release of a report on that basis. We regularly have published dozens of reports that delve into the Department's rationale for specific policies and decisions, and comment on the basis and process on which those decisions were made.

Question 5. I have to say, I find it disturbing that this report, which was made necessary by the secrecy and confusion surrounding the implementation of the President's Muslim travel ban, is now itself mired in secrecy and confusion. At minimum, the extreme delay in releasing the report, and the unusual scope and breadth

of the redactions create the appearance that DHS and DOJ exerted improper influence over the Office of the Inspector General and sought to limit the impact of the report's critical conclusions. I think the American people deserve transparency and accountability. Mr. Kelly, will you release an un-redacted copy of this report?

Answer. While transparency and accountability are paramount to our mission, those important objectives must be balanced against other important interests, including personal privacy, national security, and law enforcement interests. As a general matter, the Department has the legal right to protect from public disclosure certain sensitive information concerning the Department's operations subject to various statutory exclusions and common law privileges. In this case, the Department has made what it claims to be good faith withholdings pursuant to these bases. Accordingly, despite continuing to believe that the Department's claims of privilege may be overbroad, we are bound to issue our report with the Department's redactions. Unless the Department decides to peel back its redactions, we will not be releasing an unredacted copy of this report.

Hiring/Recruitment.

Question 6. We have seen with Customs and Border employment that recruitment can be a challenge. Have you seen similar barriers to bringing in qualified personnel who stay long enough to keep a consistent and high-level team together on both aviation, as well as surface transportation security?

Answer. We are currently conducting an audit on TSA's efforts to hire, train and retain employees. We anticipate completing our audit by the end of the Fiscal Year and would be happy to brief your office on the results of the final report.